

NATIONAL CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION ACT OF 2014

JULY 23, 2014.—Committed to the Committee of the Whole House on the State of
the Union and ordered to be printed

Mr. McCAUL, from the Committee on Homeland Security,
submitted the following

R E P O R T

[To accompany H.R. 3696]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security, to whom was referred the bill (H.R. 3696) to amend the Homeland Security Act of 2002 to make certain improvements regarding cybersecurity and critical infrastructure protection, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

Purpose and Summary	Page 19
Background and Need for Legislation	19
Hearings	22
Committee Consideration	24
Committee Votes	26
Committee Oversight Findings	27
New Budget Authority, Entitlement Authority, and Tax Expenditures	27
Congressional Budget Office Estimate	27
Statement of General Performance Goals and Objectives	30
Congressional Earmarks, Limited Tax Benefits, and Limited Tariff Benefits ...	30
Federal Mandates Statement	30
Preemption Clarification	31
Advisory Committee Statement	31
Applicability to Legislative Branch	31
Section-by-Section Analysis of the Legislation	31
Changes in Existing Law Made by the Bill, as Reported	54
Committee Correspondence	77

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the “National Cybersecurity and Critical Infrastructure Protection Act of 2014”.

SEC. 2. TABLE OF CONTENTS.

The table of contents for this Act is as follows:

Sec. 1. Short title.

Sec. 2. Table of contents.

TITLE I—SECURING THE NATION AGAINST CYBER ATTACK

Sec. 101. Homeland Security Act of 2002 definitions.

Sec. 102. Enhancement of cybersecurity.

Sec. 103. Protection of critical infrastructure and information sharing.

Sec. 104. National Cybersecurity and Communications Integration Center.

Sec. 105. Cyber incident response and technical assistance.

Sec. 106. Streamlining of Department cybersecurity organization.

TITLE II—PUBLIC-PRIVATE COLLABORATION ON CYBERSECURITY

Sec. 201. Public-private collaboration on cybersecurity.

Sec. 202. SAFETY Act and qualifying cyber incidents.

Sec. 203. Prohibition on new regulatory authority.

Sec. 204. Prohibition on additional authorization of appropriations.

Sec. 205. Prohibition on collection activities to track individuals’ personally identifiable information.

Sec. 206. Cybersecurity scholars.

Sec. 207. National Research Council study on the resilience and reliability of the Nation’s power grid.

TITLE III—HOMELAND SECURITY CYBERSECURITY WORKFORCE

Sec. 301. Homeland security cybersecurity workforce.

Sec. 302. Personnel authorities.

TITLE I—SECURING THE NATION AGAINST CYBER ATTACK

SEC. 101. HOMELAND SECURITY ACT OF 2002 DEFINITIONS.

Section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101) is amended by adding at the end the following new paragraphs:

“(19) The term ‘critical infrastructure’ has the meaning given that term in section 1016(e) of the USA Patriot Act (42 U.S.C. 5195c(e)).

“(20) The term ‘critical infrastructure owner’ means a person that owns critical infrastructure.

“(21) The term ‘critical infrastructure operator’ means a critical infrastructure owner or other person that manages, runs, or operates, in whole or in part, the day-to-day operations of critical infrastructure.

“(22) The term ‘cyber incident’ means an incident, or an attempt to cause an incident, that, if successful, would—

“(A) jeopardize or imminently jeopardize, without lawful authority, the security, integrity, confidentiality, or availability of an information system or network of information systems or any information stored on, processed on, or transiting such a system or network;

“(B) constitute a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies related to such a system or network, or an act of terrorism against such a system or network;

or

“(C) result in the denial of access to or degradation, disruption, or destruction of such a system or network, or the defeat of an operations control or technical control essential to the security or operation of such a system or network.

“(23) The term ‘cybersecurity mission’ means activities that encompass the full range of threat reduction, vulnerability reduction, deterrence, incident response, resiliency, and recovery activities to foster the security and stability of cyberspace.

“(24) The term ‘cybersecurity purpose’ means the purpose of ensuring the security, integrity, confidentiality, or availability of, or safeguarding, an information system or network of information systems, including protecting such a system or network, or data residing on such a system or network, including protection of such a system or network, from—

“(A) a vulnerability of such a system or network;

“(B) a threat to the security, integrity, confidentiality, or availability of such a system or network, or any information stored on, processed on, or transiting such a system or network;

“(C) efforts to deny access to or degrade, disrupt, or destroy such a system or network; or

“(D) efforts to gain unauthorized access to such a system or network, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting such a system or network.

“(25) The term ‘cyber threat’ means any action that may result in unauthorized access to, exfiltration of, manipulation of, harm of, or impairment to the security, integrity, confidentiality, or availability of an information system or network of information systems, or information that is stored on, processed by, or transiting such a system or network.

“(26) The term ‘cyber threat information’ means information directly pertaining to—

“(A) a vulnerability of an information system or network of information systems of a government or private entity;

“(B) a threat to the security, integrity, confidentiality, or availability of such a system or network of a government or private entity, or any information stored on, processed on, or transiting such a system or network;

“(C) efforts to deny access to or degrade, disrupt, or destroy such a system or network of a government or private entity;

“(D) efforts to gain unauthorized access to such a system or network, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting such a system or network; or

“(E) an act of terrorism against an information system or network of information systems.

“(27) The term ‘Federal civilian information systems’—

“(A) means information, information systems, and networks of information systems that are owned, operated, controlled, or licensed for use by, or on behalf of, any Federal agency, including such systems or networks used or operated by another entity on behalf of a Federal agency; but

“(B) does not include—

“(i) a national security system; or

“(ii) information, information systems, and networks of information systems that are owned, operated, controlled, or licensed solely for use by, or on behalf of, the Department of Defense, a military department, or an element of the intelligence community.

“(28) The term ‘information security’ means the protection of information, information systems, and networks of information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

“(A) integrity, including guarding against improper information modification or destruction, including ensuring nonrepudiation and authenticity;

“(B) confidentiality, including preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

“(C) availability, including ensuring timely and reliable access to and use of information.

“(29) The term ‘information system’ means the underlying framework and functions used to process, transmit, receive, or store information electronically, including programmable electronic devices, communications networks, and industrial or supervisory control systems and any associated hardware, software, or data.

“(30) The term ‘private entity’ means any individual or any private or publicly-traded company, public or private utility (including a utility that is a unit of a State or local government, or a political subdivision of a State government), organization, or corporation, including an officer, employee, or agent thereof.

“(31) The term ‘shared situational awareness’ means an environment in which cyber threat information is shared in real time between all designated Federal cyber operations centers to provide actionable information about all known cyber threats.”

SEC. 102. ENHANCEMENT OF CYBERSECURITY.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002 is amended by adding at the end the following new section:

“SEC. 226. ENHANCEMENT OF CYBERSECURITY.

“The Secretary, in collaboration with the heads of other appropriate Federal Government entities, shall conduct activities for cybersecurity purposes, including the provision of shared situational awareness to each other to enable real-time, inte-

grated, and operational actions to protect from, prevent, mitigate, respond to, and recover from cyber incidents.”.

(b) CLERICAL AMENDMENTS.—

(1) SUBTITLE HEADING.—The heading for subtitle C of title II of such Act is amended to read as follows:

“Subtitle C—Cybersecurity and Information Sharing”.

(2) TABLE OF CONTENTS.—The table of contents in section 1(b) of such Act is amended—

(A) by adding after the item relating to section 225 the following new item:

“Sec. 226. Enhancement of cybersecurity.”;

and

(B) by striking the item relating to subtitle C of title II and inserting the following new item:

“Subtitle C—Cybersecurity and Information Sharing”.

SEC. 103. PROTECTION OF CRITICAL INFRASTRUCTURE AND INFORMATION SHARING.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002, as amended by section 102, is further amended by adding at the end the following new section:

“SEC. 227. PROTECTION OF CRITICAL INFRASTRUCTURE AND INFORMATION SHARING.

“(a) PROTECTION OF CRITICAL INFRASTRUCTURE.—

“(1) IN GENERAL.—The Secretary shall coordinate, on an ongoing basis, with Federal, State, and local governments, national laboratories, critical infrastructure owners, critical infrastructure operators, and other cross sector coordinating entities to—

“(A) facilitate a national effort to strengthen and maintain secure, functioning, and resilient critical infrastructure from cyber threats;

“(B) ensure that Department policies and procedures enable critical infrastructure owners and critical infrastructure operators to receive real-time, actionable, and relevant cyber threat information;

“(C) seek industry sector-specific expertise to—

“(i) assist in the development of voluntary security and resiliency strategies; and

“(ii) ensure that the allocation of Federal resources are cost effective and reduce any burden on critical infrastructure owners and critical infrastructure operators;

“(D) upon request of entities, facilitate and assist risk management efforts of such entities to reduce vulnerabilities, identify and disrupt threats, and minimize consequences to their critical infrastructure;

“(E) upon request of critical infrastructure owners or critical infrastructure operators, provide education and assistance to such owners and operators on how they may use protective measures and countermeasures to strengthen the security and resilience of the Nation’s critical infrastructure; and

“(F) coordinate a research and development strategy to facilitate and promote advancements and innovation in cybersecurity technologies to protect critical infrastructure.

“(2) ADDITIONAL RESPONSIBILITIES.—The Secretary shall—

“(A) manage Federal efforts to secure, protect, and ensure the resiliency of Federal civilian information systems using a risk-based and performance-based approach, and, upon request of critical infrastructure owners or critical infrastructure operators, support such owners’ and operators’ efforts to secure, protect, and ensure the resiliency of critical infrastructure from cyber threats;

“(B) direct an entity within the Department to serve as a Federal civilian entity by and among Federal, State, and local governments, private entities, and critical infrastructure sectors to provide multi-directional sharing of real-time, actionable, and relevant cyber threat information;

“(C) build upon existing mechanisms to promote a national awareness effort to educate the general public on the importance of securing information systems;

“(D) upon request of Federal, State, and local government entities and private entities, facilitate expeditious cyber incident response and recovery assistance, and provide analysis and warnings related to threats to and vulnerabilities of critical information systems, crisis and consequence management support, and other remote or on-site technical assistance with the heads of other appropriate Federal agencies to Federal, State, and local government entities and private entities for cyber incidents affecting critical infrastructure;

“(E) engage with international partners to strengthen the security and resilience of domestic critical infrastructure and critical infrastructure located outside of the United States upon which the United States depends; and

“(F) conduct outreach to educational institutions, including historically black colleges and universities, Hispanic serving institutions, Native American colleges, and institutions serving persons with disabilities, to encourage such institutions to promote cybersecurity awareness.

“(3) RULE OF CONSTRUCTION.—Nothing in this section may be construed to require any private entity to request assistance from the Secretary, or require any private entity requesting such assistance to implement any measure or recommendation suggested by the Secretary.

“(b) CRITICAL INFRASTRUCTURE SECTORS.—The Secretary, in collaboration with the heads of other appropriate Federal agencies, shall designate critical infrastructure sectors (that may include subdivisions of sectors within a sector as the Secretary may determine appropriate). The critical infrastructure sectors designated under this subsection may include the following:

- “(1) Chemical.
- “(2) Commercial facilities.
- “(3) Communications.
- “(4) Critical manufacturing.
- “(5) Dams.
- “(6) Defense Industrial Base.
- “(7) Emergency services.
- “(8) Energy.
- “(9) Financial services.
- “(10) Food and agriculture.
- “(11) Government facilities.
- “(12) Healthcare and public health.
- “(13) Information technology.
- “(14) Nuclear reactors, materials, and waste.
- “(15) Transportation systems.
- “(16) Water and wastewater systems.

“(17) Such other sectors as the Secretary determines appropriate.

“(c) SECTOR SPECIFIC AGENCIES.—The Secretary, in collaboration with the relevant critical infrastructure sector and the heads of other appropriate Federal agencies, shall recognize the Federal agency designated as of November 1, 2013, as the ‘Sector Specific Agency’ for each critical infrastructure sector designated under subsection (b). If the designated Sector Specific Agency for a particular critical infrastructure sector is the Department, for the purposes of this section, the Secretary shall carry out this section. The Secretary, in coordination with the heads of each such Sector Specific Agency shall—

“(1) support the security and resilience activities of the relevant critical infrastructure sector in accordance with this subtitle; and

“(2) provide institutional knowledge and specialized expertise to the relevant critical infrastructure sector.

“(d) SECTOR COORDINATING COUNCILS.—

“(1) RECOGNITION.—The Secretary, in collaboration with each critical infrastructure sector and the relevant Sector Specific Agency, shall recognize and partner with the Sector Coordinating Council for each critical infrastructure sector designated under subsection (b) to coordinate with each such sector on security and resilience activities and emergency response and recovery efforts.

“(2) MEMBERSHIP.—

“(A) IN GENERAL.—The Sector Coordinating Council for a critical infrastructure sector designated under subsection (b) shall—

“(i) be comprised exclusively of relevant critical infrastructure owners, critical infrastructure operators, private entities, and representative trade associations for the sector;

“(ii) reflect the unique composition of each sector; and

“(iii) include relevant small, medium, and large critical infrastructure owners, critical infrastructure operators, private entities, and representative trade associations for the sector.

“(B) PROHIBITION.—No government entity with regulating authority shall be a member of the Sector Coordinating Council.

“(C) LIMITATION.—The Secretary shall have no role in the determination of the membership of a Sector Coordinating Council.

“(3) ROLES AND RESPONSIBILITIES.—The Sector Coordinating Council for a critical infrastructure sector shall—

“(A) serve as a self-governing, self-organized primary policy, planning, and strategic communications entity for coordinating with the Department, the relevant Sector-Specific Agency designated under subsection (c), and the relevant Information Sharing and Analysis Centers under subsection (e) on security and resilience activities and emergency response and recovery efforts;

“(B) establish governance and operating procedures, and designate a chairperson for the sector to carry out the activities described in this subsection;

“(C) coordinate with the Department, the relevant Information Sharing and Analysis Centers under subsection (e), and other Sector Coordinating Councils to update, maintain, and exercise the National Cybersecurity Incident Response Plan in accordance with section 229(b); and

“(D) provide any recommendations to the Department on infrastructure protection technology gaps to help inform research and development efforts at the Department.

“(e) SECTOR INFORMATION SHARING AND ANALYSIS CENTERS.—

“(1) RECOGNITION.—The Secretary, in collaboration with the relevant Sector Coordinating Council and the critical infrastructure sector represented by such Council, and in coordination with the relevant Sector Specific Agency, shall recognize at least one Information Sharing and Analysis Center for each critical infrastructure sector designated under subsection (b) for purposes of paragraph (3). No other Information Sharing and Analysis Organizations, including Information Sharing and Analysis Centers, may be precluded from having an information sharing relationship within the National Cybersecurity and Communications Integration Center established pursuant to section 228. Nothing in this subsection or any other provision of this subtitle may be construed to limit, restrict, or condition any private entity or activity utilized by, among, or between private entities.

“(2) ROLES AND RESPONSIBILITIES.—In addition to such other activities as may be authorized by law, at least one Information Sharing and Analysis Center for a critical infrastructure sector shall—

“(A) serve as an information sharing resource for such sector and promote ongoing multi-directional sharing of real-time, relevant, and actionable cyber threat information and analysis by and among such sector, the Department, the relevant Sector Specific Agency, and other critical infrastructure sector Information Sharing and Analysis Centers;

“(B) establish governance and operating procedures to carry out the activities conducted under this subsection;

“(C) serve as an emergency response and recovery operations coordination point for such sector, and upon request, facilitate cyber incident response capabilities in coordination with the Department, the relevant Sector Specific Agency and the relevant Sector Coordinating Council;

“(D) facilitate cross-sector coordination and sharing of cyber threat information to prevent related or consequential impacts to other critical infrastructure sectors;

“(E) coordinate with the Department, the relevant Sector Coordinating Council, the relevant Sector Specific Agency, and other critical infrastructure sector Information Sharing and Analysis Centers on the development, integration, and implementation of procedures to support technology neutral, real-time information sharing capabilities and mechanisms within the National Cybersecurity and Communications Integration Center established pursuant to section 228, including—

“(i) the establishment of a mechanism to voluntarily report identified vulnerabilities and opportunities for improvement;

“(ii) the establishment of metrics to assess the effectiveness and timeliness of the Department’s and Information Sharing and Analysis Centers’ information sharing capabilities; and

“(iii) the establishment of a mechanism for anonymous suggestions and comments;

“(F) implement an integration and analysis function to inform sector planning, risk mitigation, and operational activities regarding the protection of each critical infrastructure sector from cyber incidents;

“(G) combine consequence, vulnerability, and threat information to share actionable assessments of critical infrastructure sector risks from cyber incidents;

“(H) coordinate with the Department, the relevant Sector Specific Agency, and the relevant Sector Coordinating Council to update, maintain, and exercise the National Cybersecurity Incident Response Plan in accordance with section 229(b); and

“(I) safeguard cyber threat information from unauthorized disclosure.

“(3) FUNDING.—Of the amounts authorized to be appropriated for each of fiscal years 2014, 2015, and 2016 for the Cybersecurity and Communications Office of the Department, the Secretary is authorized to use not less than \$25,000,000 for any such year for operations support at the National Cybersecurity and Communications Integration Center established under section 228(a) of all recognized Information Sharing and Analysis Centers under paragraph (1) of this subsection.

“(f) CLEARANCES.—The Secretary—

“(1) shall expedite the process of security clearances under Executive Order 13549 or successor orders for appropriate representatives of Sector Coordinating Councils and the critical infrastructure sector Information Sharing and Analysis Centers; and

“(2) may so expedite such processing to—

“(A) appropriate personnel of critical infrastructure owners and critical infrastructure operators; and

“(B) any other person as determined by the Secretary.

“(g) PUBLIC-PRIVATE COLLABORATION.—The Secretary, in collaboration with the critical infrastructure sectors designated under subsection (b), such sectors’ Sector Specific Agencies recognized under subsection (c), and the Sector Coordinating Councils recognized under subsection (d), shall—

“(1) conduct an analysis and review of the existing public-private partnership model and evaluate how the model between the Department and critical infrastructure owners and critical infrastructure operators can be improved to ensure the Department, critical infrastructure owners, and critical infrastructure operators are equal partners and regularly collaborate on all programs and activities of the Department to protect critical infrastructure;

“(2) develop and implement procedures to ensure continuous, collaborative, and effective interactions between the Department, critical infrastructure owners, and critical infrastructure operators; and

“(3) ensure critical infrastructure sectors have a reasonable period for review and comment of all jointly produced materials with the Department.

“(h) PROTECTION OF FEDERAL CIVILIAN INFORMATION SYSTEMS.—

“(1) IN GENERAL.—The Secretary shall administer the operational information security activities and functions to protect and ensure the resiliency of all Federal civilian information systems.

“(2) ROLES AND RESPONSIBILITIES.—The Secretary, in coordination with the heads of other Federal civilian agencies, shall—

“(A) develop, issue, and oversee the implementation and compliance of all operational information security policies and procedures to protect and ensure the resiliency of Federal civilian information systems;

“(B) administer Federal Government-wide efforts to develop and provide adequate, risk-based, cost-effective, and technology neutral information security capabilities;

“(C) establish and sustain continuous diagnostics systems for Federal civilian information systems to aggregate data and identify and prioritize the mitigation of cyber vulnerabilities in such systems for cybersecurity purposes;

“(D) develop, acquire, and operate an integrated and consolidated system of intrusion detection, analytics, intrusion prevention, and other information sharing and protective capabilities to defend Federal civilian information systems from cyber threats;

“(E) develop and conduct targeted risk assessments and operational evaluations of Federal civilian information systems, in consultation with government and private entities that own and operate such information systems, including threat, vulnerability, and impact assessments and penetration testing;

“(F) develop and provide technical assistance and cyber incident response capabilities to secure and ensure the resilience of Federal civilian information systems;

“(G) review annually the operational information security activities and functions of each of the Federal civilian agencies;

“(H) develop minimum technology neutral operational requirements for network and security operations centers to facilitate the protection of all Federal civilian information systems;

“(I) develop reporting requirements, consistent with relevant law, to ensure the National Cybersecurity and Communications Integration Center established pursuant to section 228 receives all actionable cyber threat information identified on Federal civilian information systems;

“(J) develop technology neutral performance requirements and metrics for the security of Federal civilian information systems;

“(K) implement training requirements that include industry recognized certifications to ensure that Federal civilian agencies are able to fully and timely comply with policies and procedures issued by the Secretary under this subsection; and

“(L) develop training requirements regarding privacy, civil rights, civil liberties, and information oversight for information security employees who operate Federal civilian information systems.

“(3) USE OF CERTAIN COMMUNICATIONS.—

“(A) IN GENERAL.—The Secretary may enter into contracts or other agreements, or otherwise request and obtain, in accordance with applicable law, the assistance of private entities that provide electronic communication services, remote computing services, or cybersecurity services to acquire, intercept, retain, use, and disclose communications and other system traffic, deploy countermeasures, or otherwise operate protective capabilities in accordance with subparagraphs (C), (D), (E), and (F) of paragraph (2). No cause of action shall exist against private entities for assistance provided to the Secretary in accordance with this subsection.

“(B) RULE OF CONSTRUCTION.—Nothing in subparagraph (A) may be construed to—

“(i) require or compel any private entity to enter in a contract or agreement described in such subparagraph; or

“(ii) authorize the Secretary to take any action with respect to any communications or system traffic transiting or residing on any information system or network of information systems other than a Federal civilian information system.

“(i) RECOMMENDATIONS REGARDING NEW AGREEMENTS.—Not later than 180 days after the date of the enactment of this section, the Secretary shall submit to the appropriate congressional committees recommendations on how to expedite the implementation of information sharing agreements for cybersecurity purposes between the Secretary and critical information owners and critical infrastructure operators and other private entities. Such recommendations shall address the development and utilization of a scalable form that retains all privacy and other protections in such agreements in existence as of such date, including Cooperative and Research Development Agreements. Such recommendations should also include any additional authorities or resources that may be needed to carry out the implementation of any such new agreements.

“(j) RULE OF CONSTRUCTION.—No provision of this title may be construed as modifying, limiting, or otherwise affecting the authority of any other Federal agency under any other provision of law.”.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by adding after the item relating to section 226 (as added by section 102) the following new item:

“Sec. 227. Protection of critical infrastructure and information sharing.”.

SEC. 104. NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002, as amended by sections 102 and 103, is further amended by adding at the end the following new section:

“SEC. 228. NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.

“(a) ESTABLISHMENT.—There is established in the Department the National Cybersecurity and Communications Integration Center (referred to in this section as the ‘Center’), which shall be a Federal civilian information sharing interface that provides shared situational awareness to enable real-time, integrated, and operational actions across the Federal Government, and share cyber threat information by and among Federal, State, and local government entities, Information Sharing and Analysis Centers, private entities, and critical infrastructure owners and critical infrastructure operators that have an information sharing relationship with the Center.

“(b) COMPOSITION.—The Center shall include each of the following entities:

“(1) At least one Information Sharing and Analysis Center established under section 227(e) for each critical infrastructure sector.

“(2) The Multi-State Information Sharing and Analysis Center to collaborate with State and local governments.

“(3) The United States Computer Emergency Readiness Team to coordinate cyber threat information sharing, proactively manage cyber risks to the United States, collaboratively respond to cyber incidents, provide technical assistance to information system owners and operators, and disseminate timely notifications regarding current and potential cyber threats and vulnerabilities.

“(4) The Industrial Control System Cyber Emergency Response Team to coordinate with industrial control systems owners and operators and share industrial control systems-related security incidents and mitigation measures.

“(5) The National Coordinating Center for Telecommunications to coordinate the protection, response, and recovery of national security emergency communications.

“(6) Such other Federal, State, and local government entities, private entities, organizations, or individuals as the Secretary may consider appropriate that agree to be included.

“(c) CYBER INCIDENT.—In the event of a cyber incident, the Secretary may grant the entities referred to in subsection (a) immediate temporary access to the Center as a situation may warrant.

“(d) ROLES AND RESPONSIBILITIES.—The Center shall—

“(1) promote ongoing multi-directional sharing by and among the entities referred to in subsection (a) of timely and actionable cyber threat information and analysis on a real-time basis that includes emerging trends, evolving threats, incident reports, intelligence information, risk assessments, and best practices;

“(2) coordinate with other Federal agencies to streamline and reduce redundant reporting of cyber threat information;

“(3) provide, upon request, timely technical assistance and crisis management support to Federal, State, and local government entities and private entities that own or operate information systems or networks of information systems to protect from, prevent, mitigate, respond to, and recover from cyber incidents;

“(4) facilitate cross-sector coordination and sharing of cyber threat information to prevent related or consequential impacts to other critical infrastructure sectors;

“(5) collaborate and facilitate discussions with Sector Coordinating Councils, Information Sharing and Analysis Centers, Sector Specific Agencies, and relevant critical infrastructure sectors on the development of prioritized Federal response efforts, if necessary, to support the defense and recovery of critical infrastructure from cyber incidents;

“(6) collaborate with the Sector Coordinating Councils, Information Sharing and Analysis Centers, Sector Specific Agencies, and the relevant critical infrastructure sectors on the development and implementation of procedures to support technology neutral real-time information sharing capabilities and mechanisms;

“(7) collaborate with the Sector Coordinating Councils, Information Sharing and Analysis Centers, Sector Specific Agencies, and the relevant critical infrastructure sectors to identify requirements for data and information formats and accessibility, system interoperability, and redundant systems and alternative capabilities in the event of a disruption in the primary information sharing capabilities and mechanisms at the Center;

“(8) within the scope of relevant treaties, cooperate with international partners to share information and respond to cyber incidents;

“(9) safeguard sensitive cyber threat information from unauthorized disclosure;

“(10) require other Federal civilian agencies to—

“(A) send reports and information to the Center about cyber incidents, threats, and vulnerabilities affecting Federal civilian information systems and critical infrastructure systems and, in the event a private vendor product or service of such an agency is so implicated, the Center shall first notify such private vendor of the vulnerability before further disclosing such information;

“(B) provide to the Center cyber incident detection, analysis, mitigation, and response information; and

“(C) immediately send and disclose to the Center cyber threat information received by such agencies;

“(11) perform such other duties as the Secretary may require to facilitate a national effort to strengthen and maintain secure, functioning, and resilient critical infrastructure from cyber threats;

“(12) implement policies and procedures to—

“(A) provide technical assistance to Federal civilian agencies to prevent and respond to data breaches involving unauthorized acquisition or access of personally identifiable information that occur on Federal civilian information systems;

“(B) require Federal civilian agencies to notify the Center about data breaches involving unauthorized acquisition or access of personally identifiable information that occur on Federal civilian information systems not later than two business days after the discovery of such a breach; and

“(C) require Federal civilian agencies to notify all potential victims of a data breach involving unauthorized acquisition or access of personally identifiable information that occur on Federal civilian information systems without unreasonable delay consistent with the needs of law enforcement; and

“(13) participate in exercises run by the Department’s National Exercise Program, where appropriate.

“(e) INTEGRATION AND ANALYSIS.—The Center, in coordination with the Office of Intelligence and Analysis of the Department, shall maintain an integration and analysis function, which shall —

“(1) integrate and analyze all cyber threat information received from other Federal agencies, State and local governments, Information Sharing and Analysis Centers, private entities, critical infrastructure owners, and critical infrastructure operators, and share relevant information in near real-time;

“(2) on an ongoing basis, assess and evaluate consequence, vulnerability, and threat information to share with the entities referred to in subsection (a) actionable assessments of critical infrastructure sector risks from cyber incidents and to assist critical infrastructure owners and critical infrastructure operators by making recommendations to facilitate continuous improvements to the security and resiliency of the critical infrastructure of the United States;

“(3) facilitate cross-sector integration, identification, and analysis of key interdependencies to prevent related or consequential impacts to other critical infrastructure sectors;

“(4) collaborate with the Information Sharing and Analysis Centers to tailor the analysis of information to the specific characteristics and risk to a relevant critical infrastructure sector; and

“(5) assess and evaluate consequence, vulnerability, and threat information regarding cyber incidents in coordination with the Office of Emergency Communications of the Department to help facilitate continuous improvements to the security and resiliency of public safety communications networks.

“(f) REPORT OF CYBER ATTACKS AGAINST FEDERAL GOVERNMENT NETWORKS.—The Secretary shall submit to the Committee on Homeland Security of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Comptroller General of the United States an annual report that summarizes major cyber incidents involving Federal civilian agency information systems and provides aggregate statistics on the number of breaches, the extent of any personally identifiable information that was involved, the volume of data exfiltrated, the consequential impact, and the estimated cost of remedying such breaches.

“(g) REPORT ON THE OPERATIONS OF THE CENTER.—The Secretary, in consultation with the Sector Coordinating Councils and appropriate Federal Government entities, shall submit to the Committee on Homeland Security of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Comptroller General of the United States an annual report on—

“(1) the capability and capacity of the Center to carry out its cybersecurity mission in accordance with this section, and sections 226, 227, 229, 230, 230A, and 230B;

“(2) the extent to which the Department is engaged in information sharing with each critical infrastructure sector designated under section 227(b), including—

“(A) the extent to which each such sector has representatives at the Center; and

“(B) the extent to which critical infrastructure owners and critical infrastructure operators of each critical infrastructure sector participate in information sharing at the Center;

“(3) the volume and range of activities with respect to which the Secretary collaborated with the Sector Coordinating Councils and the Sector-Specific Agencies to promote greater engagement with the Center; and

“(4) the volume and range of voluntary technical assistance sought and provided by the Department to each critical infrastructure owner and critical infrastructure operator.”.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by adding after the item relating to section 227 (as added by section 103) the following new item:

“Sec. 228. National Cybersecurity and Communications Integration Center.”.

(c) GAO REPORT.—Not later than one year after the date of the enactment of this Act, the Comptroller General of the United States shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the effectiveness of the National Cybersecurity and Communications Integration Center established under section 228 of the Homeland Security Act of 2002, as added by subsection (a) of this section, in carrying out its cybersecurity mission (as such term is defined in section 2 of the Homeland Security Act of 2002, as amended by section 101) in accordance with this Act and such section 228 and sections 226, 227, 229, 230, 230A, and 230B of the Homeland Security Act of 2002, as added by this Act.

SEC. 105. CYBER INCIDENT RESPONSE AND TECHNICAL ASSISTANCE.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002, as amended by sections 102, 103, and 104, is further amended by adding at the end the following new section:

“SEC. 229. CYBER INCIDENT RESPONSE AND TECHNICAL ASSISTANCE.

“(a) IN GENERAL.—The Secretary shall establish Cyber Incident Response Teams to—

“(1) upon request, provide timely technical assistance and crisis management support to Federal, State, and local government entities, private entities, and critical infrastructure owners and critical infrastructure operators involving cyber incidents affecting critical infrastructure; and

“(2) upon request, provide actionable recommendations on security and resilience measures and countermeasures to Federal, State, and local government entities, private entities, and critical infrastructure owners and critical infrastructure operators prior to, during, and after cyber incidents.

“(b) COORDINATION.—In carrying out subsection (a), the Secretary shall coordinate with the relevant Sector Specific Agencies, if applicable.

“(c) CYBER INCIDENT RESPONSE PLAN.—The Secretary, in coordination with the Sector Coordinating Councils, Information Sharing and Analysis Centers, and Federal, State, and local governments, shall develop, regularly update, maintain, and exercise a National Cybersecurity Incident Response Plan which shall—

“(1) include effective emergency response plans associated with cyber threats to critical infrastructure, information systems, or networks of information systems;

“(2) ensure that such National Cybersecurity Incident Response Plan can adapt to and reflect a changing cyber threat environment, and incorporate best practices and lessons learned from regular exercises, training, and after-action reports; and

“(3) facilitate discussions on the best methods for developing innovative and useful cybersecurity exercises for coordinating between the Department and each of the critical infrastructure sectors designated under section 227(b).

“(d) UPDATE TO CYBER INCIDENT ANNEX TO THE NATIONAL RESPONSE FRAMEWORK.—The Secretary, in coordination with the heads of other Federal agencies and in accordance with the National Cybersecurity Incident Response Plan under subsection (c), shall regularly update, maintain, and exercise the Cyber Incident Annex to the National Response Framework of the Department.”.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by adding after the item relating to section 228 (as added by section 104) the following new item:

“Sec. 229. Cyber incident response and technical assistance.”.

SEC. 106. STREAMLINING OF DEPARTMENT CYBERSECURITY ORGANIZATION.

(a) CYBERSECURITY AND INFRASTRUCTURE PROTECTION DIRECTORATE.—The National Protection and Programs Directorate of the Department of Homeland Security shall, after the date of the enactment of this Act, be known and designated as the “Cybersecurity and Infrastructure Protection Directorate”. Any reference to the National Protection and Programs Directorate of the Department in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Cybersecurity and Infrastructure Protection Directorate of the Department.

(b) SENIOR LEADERSHIP OF THE CYBERSECURITY AND INFRASTRUCTURE PROTECTION DIRECTORATE.—

(1) IN GENERAL.—Paragraph (1) of section 103(a) of the Homeland Security Act of 2002 (6 U.S.C. 113(a)) is amended by adding at the end the following new subparagraphs:

“(K) Under Secretary for Cybersecurity and Infrastructure Protection.

“(L) Deputy Under Secretary for Cybersecurity.

“(M) Deputy Under Secretary for Infrastructure Protection.”.

(2) CONTINUATION IN OFFICE.—The individuals who hold the positions referred to in subparagraphs (K), (L), and (M) of subsection (a) of section 103 of the Homeland Security Act of 2002 (as added by paragraph (1) of this subsection) as of the date of the enactment of this Act may continue to hold such positions.

(c) REPORT ON IMPROVING THE CAPABILITY AND EFFECTIVENESS OF THE CYBERSECURITY AND COMMUNICATIONS OFFICE.—To improve the operational capability and effectiveness in carrying out the cybersecurity mission (as such term is defined in section 2 of the Homeland Security Act of 2002, as amended by section 101) of the Department of Homeland Security, the Secretary of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on—

(1) the feasibility of making the Cybersecurity and Communications Office of the Department an operational component of the Department;

(2) recommendations for restructuring the SAFETY Act Office within the Department to protect and maintain operations in accordance with the Office’s mission to provide incentives for the development and deployment of anti-terrorism technologies while elevating the profile and mission of the Office, including the feasibility of utilizing third-party registrars for improving the throughput and effectiveness of the certification process.

(d) REPORT ON CYBERSECURITY ACQUISITION CAPABILITIES.—The Secretary of Homeland Security shall assess the effectiveness of the Department of Homeland Security’s acquisition processes and the use of existing authorities for acquiring cybersecurity technologies to ensure that such processes and authorities are capable of meeting the needs and demands of the Department’s cybersecurity mission (as such term is defined in section 2 of the Homeland Security Act of 2002, as amended by section 101). Not later than 180 days after the date of the enactment of this Act, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the effectiveness of the Department’s acquisition processes for cybersecurity technologies.

(e) RESOURCE INFORMATION.—The Secretary of Homeland Security shall make available Department of Homeland Security contact information to serve as a resource for Sector Coordinating Councils and critical infrastructure owners and critical infrastructure operators to better coordinate cybersecurity efforts with the Department relating to emergency response and recovery efforts for cyber incidents.

TITLE II—PUBLIC-PRIVATE COLLABORATION ON CYBERSECURITY

SEC. 201. PUBLIC-PRIVATE COLLABORATION ON CYBERSECURITY.

(a) NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY.—

(1) IN GENERAL.—The Director of the National Institute of Standards and Technology, in coordination with the Secretary of Homeland Security, shall, on an ongoing basis, facilitate and support the development of a voluntary, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to reduce cyber risks to critical infrastructure. The Director, in coordination with the Secretary—

(A) shall—

(i) coordinate closely and continuously with relevant private entities, critical infrastructure owners and critical infrastructure operators, Sector Coordinating Councils, Information Sharing and Analysis Centers, and other relevant industry organizations, and incorporate industry expertise to the fullest extent possible;

(ii) consult with the Sector Specific Agencies, Federal, State and local governments, the governments of other countries, and international organizations;

(iii) utilize a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, that may be voluntarily adopted by critical infrastructure

owners and critical infrastructure operators to help them identify, assess, and manage cyber risks;

(iv) include methodologies to—

(I) identify and mitigate impacts of the cybersecurity measures or controls on business confidentiality; and

(II) protect individual privacy and civil liberties;

(v) incorporate voluntary consensus standards and industry best practices, and align with voluntary international standards to the fullest extent possible;

(vi) prevent duplication of existing regulatory processes and prevent conflict with or superseding of existing regulatory requirements and processes; and

(vii) include such other similar and consistent elements as determined necessary; and

(B) shall not prescribe or otherwise require—

(i) the use of specific solutions;

(ii) the use of specific information technology products or services; or

(iii) that information technology products or services be designed, developed, or manufactured in a particular manner.

(2) LIMITATION.—Information shared with or provided to the Director of the National Institute of Standards and Technology or the Secretary of Homeland Security for the purpose of the activities under paragraph (1) may not be used by any Federal, State, or local government department or agency to regulate the activity of any private entity.

(b) AMENDMENT.—

(1) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002, as amended by sections 102, 103, 104, and 105, is further amended by adding at the end the following new section:

“SEC. 230. PUBLIC-PRIVATE COLLABORATION ON CYBERSECURITY.

“(a) MEETINGS.—The Secretary shall meet with the Sector Coordinating Council for each critical infrastructure sector designated under section 227(b) on a biannual basis to discuss the cybersecurity threat to critical infrastructure, voluntary activities to address cybersecurity, and ideas to improve the public-private partnership to enhance cybersecurity, in which the Secretary shall—

“(1) provide each Sector Coordinating Council an assessment of the cybersecurity threat to each critical infrastructure sector designated under section 227(b), including information relating to—

“(A) any actual or assessed cyber threat, including a consideration of adversary capability and intent, preparedness, target attractiveness, and deterrence capabilities;

“(B) the extent and likelihood of death, injury, or serious adverse effects to human health and safety caused by an act of terrorism or other disruption, destruction, or unauthorized use of critical infrastructure;

“(C) the threat to national security caused by an act of terrorism or other disruption, destruction, or unauthorized use of critical infrastructure; and

“(D) the harm to the economy that would result from an act of terrorism or other disruption, destruction, or unauthorized use of critical infrastructure; and

“(2) provide recommendations, which may be voluntarily adopted, on ways to improve cybersecurity of critical infrastructure.

“(b) REPORT.—

“(1) IN GENERAL.—Starting 30 days after the end of the fiscal year in which the National Cybersecurity and Critical Infrastructure Protection Act of 2013 is enacted and annually thereafter, the Secretary shall submit to the appropriate congressional committees a report on the state of cybersecurity for each critical infrastructure sector designated under section 227(b) based on discussions between the Department and the Sector Coordinating Council in accordance with subsection (a) of this section. The Secretary shall maintain a public copy of each report, and each report may include a non-public annex for proprietary, business-sensitive information, or other sensitive information. Each report shall include, at a minimum information relating to—

“(A) the risk to each critical infrastructure sector, including known cyber threats, vulnerabilities, and potential consequences;

“(B) the extent and nature of any cybersecurity incidents during the previous year, including the extent to which cyber incidents jeopardized or imminently jeopardized information systems;

“(C) the current status of the voluntary, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to reduce cyber risks within each critical infrastructure sector; and

“(D) the volume and range of voluntary technical assistance sought and provided by the Department to each critical infrastructure sector.

“(2) SECTOR COORDINATING COUNCIL RESPONSE.—Before making public and submitting each report required under paragraph (1), the Secretary shall provide a draft of each report to the Sector Coordinating Council for the critical infrastructure sector covered by each such report. The Sector Coordinating Council at issue may provide to the Secretary a written response to such report within 45 days of receiving the draft. If such Sector Coordinating Council provides a written response, the Secretary shall include such written response in the final version of each report required under paragraph (1).

“(c) LIMITATION.—Information shared with or provided to a Sector Coordinating Council, a critical infrastructure sector, or the Secretary for the purpose of the activities under subsections (a) and (b) may not be used by any Federal, State, or local government department or agency to regulate the activity of any private entity.”.

(2) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by adding after the item relating to section 229 (as added by section 105) the following new item:

“Sec. 230. Public-private collaboration on cybersecurity.”.

SEC. 202. SAFETY ACT AND QUALIFYING CYBER INCIDENTS.

(a) IN GENERAL.—The Support Anti-Terrorism By Fostering Effective Technologies Act of 2002 (6 U.S.C. 441 et seq.) is amended—

(1) in section 862(b) (6 U.S.C. 441(b))—

(A) in the heading, by striking “DESIGNATION OF QUALIFIED ANTI-TERRORISM TECHNOLOGIES” and inserting “DESIGNATION OF ANTI-TERRORISM AND CYBERSECURITY TECHNOLOGIES”;

(B) in the matter preceding paragraph (1), by inserting “and cybersecurity” after “anti-terrorism”;

(C) in paragraphs (3), (4), and (5), by inserting “or cybersecurity” after “anti-terrorism” each place it appears; and

(D) in paragraph (7)—

(i) by inserting “or cybersecurity technology” after “Anti-terrorism technology”; and

(ii) by inserting “or qualifying cyber incidents” after “acts of terrorism”;

(2) in section 863 (6 U.S.C. 442)—

(A) by inserting “or cybersecurity” after “anti-terrorism” each place it appears;

(B) by inserting “or qualifying cyber incident” after “act of terrorism” each place it appears; and

(C) by inserting “or qualifying cyber incidents” after “acts of terrorism” each place it appears;

(3) in section 864 (6 U.S.C. 443)—

(A) by inserting “or cybersecurity” after “anti-terrorism” each place it appears; and

(B) by inserting “or qualifying cyber incident” after “act of terrorism” each place it appears; and

(4) in section 865 (6 U.S.C. 444)—

(A) in paragraph (1)—

(i) in the heading, by inserting “OR CYBERSECURITY” after “ANTI-TERRORISM”;

(ii) by inserting “or cybersecurity” after “anti-terrorism”;

(iii) by inserting “or qualifying cyber incidents” after “acts of terrorism”;

(iv) by inserting “or incidents” after “such acts”; and

(B) by adding at the end the following new paragraph:

“(7) QUALIFYING CYBER INCIDENT.—

“(A) IN GENERAL.—The term ‘qualifying cyber incident’ means any act that the Secretary determines meets the requirements under subparagraph (B), as such requirements are further defined and specified by the Secretary.

“(B) REQUIREMENTS.—A qualifying cyber incident meets the requirements of this subparagraph if—

“(i) the incident is unlawful or otherwise exceeds authorized access authority;

“(ii) the incident disrupts or imminently jeopardizes the integrity, operation, confidentiality, or availability of programmable electronic devices, communication networks, including hardware, software and data that are essential to their reliable operation, electronic storage devices, or any other information system, or the information that system controls, processes, stores, or transmits;

“(iii) the perpetrator of the incident gains access to an information system or a network of information systems resulting in—

“(I) misappropriation or theft of data, assets, information, or intellectual property;

“(II) corruption of data, assets, information, or intellectual property;

“(III) operational disruption; or

“(IV) an adverse effect on such system or network, or the data, assets, information, or intellectual property contained therein; and

“(iv) the incident causes harm inside or outside the United States that results in material levels of damage, disruption, or casualties severely affecting the United States population, infrastructure, economy, or national morale, or Federal, State, local, or tribal government functions.

“(C) **RULE OF CONSTRUCTION.**—For purposes of clause (iv) of subparagraph (B), the term ‘severely’ includes any qualifying cyber incident, whether at a local, regional, state, national, international, or tribal level, that affects—

“(i) the United States population, infrastructure, economy, or national morale, or

“(ii) Federal, State, local, or tribal government functions.”.

(b) **FUNDING.**—Of the amounts authorized to be appropriated for each of fiscal years 2014, 2015, and 2016 for the Department of Homeland Security, the Secretary of Homeland Security is authorized to use not less than \$20,000,000 for any such year for the Department’s SAFETY Act Office.

SEC. 203. PROHIBITION ON NEW REGULATORY AUTHORITY.

This Act and the amendments made by this Act (except that this section shall not apply in the case of section 202 of this Act and the amendments made by such section 202) do not—

(1) create or authorize the issuance of any new regulations or additional Federal Government regulatory authority; or

(2) permit regulatory actions that would duplicate, conflict with, or supercede existing regulatory requirements, mandatory standards, or related processes.

SEC. 204. PROHIBITION ON ADDITIONAL AUTHORIZATION OF APPROPRIATIONS.

No additional funds are authorized to be appropriated to carry out this Act and the amendments made by this Act. This Act and such amendments shall be carried out using amounts otherwise available for such purposes.

SEC. 205. PROHIBITION ON COLLECTION ACTIVITIES TO TRACK INDIVIDUALS’ PERSONALLY IDENTIFIABLE INFORMATION.

Nothing in this Act shall permit the Department of Homeland Security to engage in the monitoring, surveillance, exfiltration, or other collection activities for the purpose of tracking an individual’s personally identifiable information.

SEC. 206. CYBERSECURITY SCHOLARS.

The Secretary of Homeland Security shall determine the feasibility and potential benefit of developing a visiting security researchers program from academia, including cybersecurity scholars at the Department of Homeland Security’s Centers of Excellence, as designated by the Secretary, to enhance knowledge with respect to the unique challenges of addressing cyber threats to critical infrastructure. Eligible candidates shall possess necessary security clearances and have a history of working with Federal agencies in matters of national or domestic security.

SEC. 207. NATIONAL RESEARCH COUNCIL STUDY ON THE RESILIENCE AND RELIABILITY OF THE NATION’S POWER GRID.

(a) **INDEPENDENT STUDY.**—Not later than 60 days after the date of the enactment of this Act, the Secretary of Homeland Security, in coordination with the heads of other departments and agencies, as necessary, shall enter into an agreement with the National Research Council to conduct research of the future resilience and reliability of the Nation’s electric power transmission and distribution system. The research under this subsection shall be known as the “Saving More American Resources Today Study” or the “SMART Study”. In conducting such research, the National Research Council shall—

(1) research the options for improving the Nation's ability to expand and strengthen the capabilities of the Nation's power grid, including estimation of the cost, time scale for implementation, and identification of the scale and scope of any potential significant health and environmental impacts;

(2) consider the forces affecting the grid, including technical, economic, regulatory, environmental, and geopolitical factors, and how such forces are likely to affect—

(A) the efficiency, control, reliability and robustness of operation;

(B) the ability of the grid to recover from disruptions, including natural disasters and terrorist attacks;

(C) the ability of the grid to incorporate greater reliance on distributed and intermittent power generation and electricity storage;

(D) the ability of the grid to adapt to changing patterns of demand for electricity; and

(E) the economic and regulatory factors affecting the evolution of the grid;

(3) review Federal, State, industry, and academic research and development programs and identify technological options that could improve the future grid;

(4) review the implications of increased reliance on digital information and control of the power grid for improving reliability, resilience, and congestion and for potentially increasing vulnerability to cyber attack;

(5) review regulatory, industry, and institutional factors and programs affecting the future of the grid;

(6) research the costs and benefits, as well as the strengths and weaknesses, of the options identified under paragraph (1) to address the emerging forces described in paragraph (2) that are shaping the grid;

(7) identify the barriers to realizing the options identified and suggest strategies for overcoming those barriers including suggested actions, priorities, incentives, and possible legislative and executive actions; and

(8) research the ability of the grid to integrate existing and future infrastructure, including utilities, telecommunications lines, highways, and other critical infrastructure.

(b) COOPERATION AND ACCESS TO INFORMATION AND PERSONNEL.—The Secretary shall ensure that the National Research Council receives full and timely cooperation, including full access to information and personnel, from the Department of Homeland Security, the Department of Energy, including the management and operating components of the Departments, and other Federal departments and agencies, as necessary, for the purposes of conducting the study described in subsection (a).

(c) REPORT.—

(1) IN GENERAL.—Not later than 18 months from the date on which the Secretary enters into the agreement with the National Research Council described in subsection (a), the National Research Council shall submit to the Secretary and the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report containing the findings of the research required by that subsection.

(2) FORM OF REPORT.—The report under paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

(d) FUNDING.—Of the amounts authorized to be appropriated for 2014 for the Department of Homeland Security, the Secretary of Homeland Security is authorized to obligate and expend not more than \$2,000,000 for the National Research Council report.

TITLE III—HOMELAND SECURITY CYBERSECURITY WORKFORCE

SEC. 301. HOMELAND SECURITY CYBERSECURITY WORKFORCE.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002, as amended by sections 101, 102, 103, 104, 105, and 201, is further amended by adding at the end the following new section:

“SEC. 230A. CYBERSECURITY OCCUPATION CATEGORIES, WORKFORCE ASSESSMENT, AND STRATEGY.

“(a) SHORT TITLE.—This section may be cited as the ‘Homeland Security Cybersecurity Boots-on-the-Ground Act’.

“(b) CYBERSECURITY OCCUPATION CATEGORIES.—

“(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this section, the Secretary shall develop and issue comprehensive occupation

categories for individuals performing activities in furtherance of the cybersecurity mission of the Department.

“(2) APPLICABILITY.—The Secretary shall ensure that the comprehensive occupation categories issued under paragraph (1) are used throughout the Department and are made available to other Federal agencies.

“(c) CYBERSECURITY WORKFORCE ASSESSMENT.—

“(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this section and annually thereafter, the Secretary shall assess the readiness and capacity of the workforce of the Department to meet its cybersecurity mission.

“(2) CONTENTS.—The assessment required under paragraph (1) shall, at a minimum, include the following:

“(A) Information where cybersecurity positions are located within the Department, specified in accordance with the cybersecurity occupation categories issued under subsection (b).

“(B) Information on which cybersecurity positions are—

“(i) performed by—

“(I) permanent full time departmental employees, together with demographic information about such employees’ race, ethnicity, gender, disability status, and veterans status;

“(II) individuals employed by independent contractors; and

“(III) individuals employed by other Federal agencies, including the National Security Agency; and

“(ii) vacant.

“(C) The number of individuals hired by the Department pursuant to the authority granted to the Secretary in 2009 to permit the Secretary to fill 1,000 cybersecurity positions across the Department over a three year period, and information on what challenges, if any, were encountered with respect to the implementation of such authority.

“(D) Information on vacancies within the Department’s cybersecurity supervisory workforce, from first line supervisory positions through senior departmental cybersecurity positions.

“(E) Information on the percentage of individuals within each cybersecurity occupation category who received essential training to perform their jobs, and in cases in which such training is not received, information on what challenges, if any, were encountered with respect to the provision of such training.

“(F) Information on recruiting costs incurred with respect to efforts to fill cybersecurity positions across the Department in a manner that allows for tracking of overall recruiting and identifying areas for better coordination and leveraging of resources within the Department.

“(d) WORKFORCE STRATEGY.—

“(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this section, the Secretary shall develop, maintain, and, as necessary, update, a comprehensive workforce strategy that enhances the readiness, capacity, training, recruitment, and retention of the cybersecurity workforce of the Department.

“(2) CONTENTS.—The comprehensive workforce strategy developed under paragraph (1) shall include—

“(A) a multiphased recruitment plan, including relating to experienced professionals, members of disadvantaged or underserved communities, the unemployed, and veterans;

“(B) a 5-year implementation plan;

“(C) a 10-year projection of the Department’s cybersecurity workforce needs; and

“(D) obstacles impeding the hiring and development of a cybersecurity workforce at the Department.

“(e) INFORMATION SECURITY TRAINING.—Not later than 270 days after the date of the enactment of this section, the Secretary shall establish and maintain a process to verify on an ongoing basis that individuals employed by independent contractors who serve in cybersecurity positions at the Department receive initial and recurrent information security training comprised of general security awareness training necessary to perform their job functions, and role-based security training that is commensurate with assigned responsibilities. The Secretary shall maintain documentation to ensure that training provided to an individual under this subsection meets or exceeds requirements for such individual’s job function.

“(f) UPDATES.—The Secretary shall submit to the appropriate congressional committees annual updates regarding the cybersecurity workforce assessment required under subsection (c), information on the progress of carrying out the comprehensive

workforce strategy developed under subsection (d), and information on the status of the implementation of the information security training required under subsection (e).

“(g) GAO STUDY.—The Secretary shall provide the Comptroller General of the United States with information on the cybersecurity workforce assessment required under subsection (c) and progress on carrying out the comprehensive workforce strategy developed under subsection (d). The Comptroller General shall submit to the Secretary and the appropriate congressional committees a study on such assessment and strategy.

“(h) CYBERSECURITY FELLOWSHIP PROGRAM.—Not later than 120 days after the date of the enactment of this section, the Secretary shall submit to the appropriate congressional committees a report on the feasibility of establishing a Cybersecurity Fellowship Program to offer a tuition payment plan for undergraduate and doctoral candidates who agree to work for the Department for an agreed-upon period of time.”.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by adding after the item relating to section 230 (as added by section 201) the following new item:

“Sec. 230A. Cybersecurity occupation categories, workforce assessment, and strategy.”.

SEC. 302. PERSONNEL AUTHORITIES.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002, as amended by sections 101, 102, 103, 104, 105, 106, 201, and 301 is further amended by adding at the end the following new section:

“SEC. 230B. PERSONNEL AUTHORITIES.

“(a) IN GENERAL.—

“(1) PERSONNEL AUTHORITIES.—The Secretary may exercise with respect to qualified employees of the Department the same authority that the Secretary of Defense has with respect to civilian intelligence personnel and the scholarship program under sections 1601, 1602, 1603, and 2200a of title 10, United States Code, to establish as positions in the excepted service, appoint individuals to such positions, fix pay, and pay a retention bonus to any employee appointed under this section if the Secretary determines that such is needed to retain essential personnel. Before announcing the payment of a bonus under this paragraph, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a written explanation of such determination. Such authority shall be exercised—

“(A) to the same extent and subject to the same conditions and limitations that the Secretary of Defense may exercise such authority with respect to civilian intelligence personnel of the Department of Defense; and

“(B) in a manner consistent with the merit system principles set forth in section 2301 of title 5, United States Code.

“(2) CIVIL SERVICE PROTECTIONS.—Sections 1221 and 2302, and chapter 75 of title 5, United States Code, shall apply to the positions established pursuant to the authorities provided under paragraph (1).

“(3) PLAN FOR EXECUTION OF AUTHORITIES.—Not later than 120 days after the date of the enactment of this section, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report that contains a plan for the use of the authorities provided under this subsection.

“(b) ANNUAL REPORT.—Not later than one year after the date of the enactment of this section and annually thereafter for four years, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a detailed report (including appropriate metrics on actions occurring during the reporting period) that discusses the processes used by the Secretary in implementing this section and accepting applications, assessing candidates, ensuring adherence to veterans’ preference, and selecting applicants for vacancies to be filled by a qualified employee.

“(c) DEFINITION OF QUALIFIED EMPLOYEE.—In this section, the term ‘qualified employee’ means an employee who performs functions relating to the security of Federal civilian information systems, critical infrastructure information systems, or networks of either of such systems.”.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by adding after the item relating to section 230A (as added by section 301) the following new item:

“Sec. 230B. Personnel authorities.”.

PURPOSE AND SUMMARY

The purpose of H.R. 3696, the “National Cybersecurity and Critical Infrastructure Protection Act of 2014” or the “NCCIP Act”, is to amend the Homeland Security Act of 2002 (Pub. L. 107–296) to make certain improvements regarding cybersecurity and critical infrastructure protection, and for other purposes.

H.R. 3696 codifies and strengthens the National Cybersecurity and Communications Integration Center (NCCIC), a Federal civilian interface to facilitate real-time cyber threat information sharing across critical infrastructure sectors.

In furtherance of fostering an effective partnership between private industry and the Department of Homeland Security (DHS or the Department), H.R. 3696 directs DHS to leverage industry-led organizations to facilitate critical infrastructure protection and incident response, as appropriate. Successful aspects of the National Infrastructure Protection Plan (NIPP), a public-private partnership framework called for in Homeland Security Presidential Directive 7 (HSPD–7), Critical Infrastructure Identification, Prioritization, and Protection, that has been supported by the private sector since 2003, are codified in this legislation. These include: (1) The roles and responsibilities of Sector Specific Agencies; (2) the formation of Sector Coordinating Councils; and (3) the establishment of Information Sharing and Analysis Centers. This public-private partnership framework was recently updated in February 2013 by Presidential Policy Directive 21 (PPD–21), Critical Infrastructure Security and Resilience.

Additionally, H.R. 3696 codifies the Department’s Cyber Incident Response Teams to provide timely technical assistance, crisis management, and actionable recommendations on cyber threats to critical infrastructure owners and operators on a voluntary basis. This ensures that a National Cybersecurity Incident Response Plan is developed and exercised, and codifies DHS operational information security activities to protect and ensure the integrity and resiliency of all Federal civilian information systems and networks operating within the “.gov” domain.

H.R. 3696 also amends the SAFETY Act (Subtitle G of the Homeland Security Act of 2002, Pub. L. 107–296) to clarify that cybersecurity technologies and services may be certified by the DHS SAFETY Act Office and establish a threshold for qualifying cyber incidents. This allows private entities can voluntarily submit their cybersecurity procedures to the SAFETY Act Office to gain additional liability protections in the event of an act of terrorism or a qualifying cyber incident.

Finally, this legislation directs the Secretary to establish cybersecurity occupation categories, assess the readiness and capacity of the Department’s cyber workforce, and develop a comprehensive strategy to enhance the readiness, capacity, training, recruitment, and retention of the Department’s cybersecurity workforce.

BACKGROUND AND NEED FOR LEGISLATION

The threat of cyber attack to both our economic and National security is significant. Each day, our Nation’s most critical digital systems are attacked and probed by our enemies, adversaries, and international competitors relentlessly looking for ways to exploit

American digital networks to disrupt and destroy our Nation's critical infrastructure, conduct cyber espionage, and steal intellectual property for financial gain. Malicious underground and state-sponsored cyber hackers are also continuing to compromise sensitive information such as credit cards, bank accounts and social security numbers.

In 2013, Mandiant released a report entitled "APT1: Exposing One of China's Cyber Espionage Units", providing detailed evidence of hackers linked to the Chinese military hacking into major U.S. companies for intellectual property and for economic espionage purposes, defense systems to steal sensitive military information, and critical infrastructure to gain access to gas lines, power grids and water systems. Additionally, Iranian-backed hackers are increasing the number of cyber attacks against U.S. companies, and in one example gained access to control system software that could allow the hackers to control, shut down, or damage oil and gas pipelines in the United States. In 2012, Iran used cyber weapons to attack Saudi Arabia's national oil company, Aramco, severely damaging 30,000 computers. The growing cyber threat from Iran is particularly concerning given its hostile intent and willingness to sabotage critical infrastructure here in the United States. In addition to cyber attacks against the energy sector, Iran continues to target major U.S. banks by using disruptive denial-of-service attacks to shut down websites and restrict Americans' ability to access their financial institutions. While other high profile retail data breaches at Target and Neiman Marcus resonate with the public, a successful cyber attack on our critical infrastructure could cause loss of life and catastrophic damage to the U.S. economy.

In January 2014, before the Senate Select Committee on Intelligence, the Director of National Intelligence, James Clapper, testified that "critical infrastructure, particularly the . . . systems used in water management, oil and gas pipelines, electrical power distribution, and mass transit, provides an enticing target to malicious actors." In November 2013, before the Senate Committee on Homeland Security and Governmental Affairs, the Director of the Federal Bureau of Investigation, James Comey, stated, "We anticipate that in the future, resources devoted to cyber-based threats will equal or even eclipse the resources devoted to non-cyber based terrorist threats. According to the Wall Street Journal, in August 2013 the Central Intelligence Agency's (CIA) Deputy Director, Michael Morell, listed cyber attacks as a top threat because U.S. adversaries are working hard to develop attack capabilities. He said, "Cyber attacks that destroy networks in the U.S. could come in the next few years" and are "the thing I worry most about in the long term."

Cybersecurity is the new frontier of our National and economic security. The U.S. needs to harden its systems and networks to become both resistant and resilient to the threat while maintaining our civil liberties and privacy protections. Cyber incidents could result in significant regional or National effects on public health or safety, economic security, and National security.

According to PPD-21, the Department of Homeland Security is responsible for coordinating the overall national protection, prevention, mitigation of, and recovery from, cyber attacks. While the Department has been building its capability to protect our Nation's

critical infrastructure from cyber attacks, H.R. 3696 seeks to codify, clarify, and enhance the Department's cybersecurity efforts while providing the necessary Congressional oversight over DHS cybersecurity programs. This legislation also provides enhanced oversight of the hundreds of millions of dollars that Congress appropriates to the Department of Homeland Security for cybersecurity purposes.

H.R. 3696 reflects extensive outreach and significant collaboration with all 16 critical infrastructure sectors, and more than 300 meetings with experts and stakeholders, including the owners and operators of critical infrastructure, government agencies, academics, and privacy and civil liberties advocates.

To address the greatest vulnerabilities and gaps in our systems, H.R. 3696 seeks to establish an effective partnership between the Department of Homeland Security and the private sector to facilitate critical infrastructure protection and resiliency efforts. This legislation also ensures that cyber incident response plans and procedures are coordinated with Federal, State, local, and private sector stakeholders and are in effect before a cyber incident takes place. With 85 percent of the Nation's critical infrastructure owned or operated by the private sector, it is essential that Government and industry continue to collaborate and work together to address the growing cybersecurity threat. Specifically, H.R. 3696 codifies the principles of the National Infrastructure Protection Plan (NIPP), a public-private partnership framework called for in Homeland Security Presidential Directive 7 (HSPD-7) and that has been supported by the private sector since 2003. This public-private partnership framework was recently updated in February 2013 in PPD-21 on Critical Infrastructure Security and Resilience. The NIPP structure has already taken root with industry and codifying it will allow it to further mature.

Prohibiting any new regulatory authorities, H.R. 3696 articulates how to address cyber vulnerabilities and gaps and develops baselines where none exist in a way that is ongoing, adaptive, risk-based, and fosters industry and government collaboration without impeding the free flow of commerce and people. With ever-evolving cybersecurity threats and regular advancements in new technologies, our Nation's cybersecurity posture needs to be both dynamic and agile, and be conducted through a cyber risk-based management approach. To better understand our Nation's cybersecurity posture, the bill requires the Department to submit to Congress an annual report on the state of cybersecurity for each critical infrastructure sector. In the spirit of partnership, the report is to be developed in collaboration with the Sector Coordinating Councils.

Additionally, this legislation enhances and fosters the groundwork laid by industry and DHS by strengthening and officially establishing the Department's civilian, transparent interface to allow real-time cyber threat information sharing across the critical infrastructure sectors. The legislation will strengthen the work that DHS is already doing and enhance the capabilities of the Department so it can realize its full potential of being the main interface for the private sector and government to facilitate the sharing of cyber threat information—in two directions. Notably, DHS has robust privacy and civil liberties offices that adhere to the Fair Information Practice Principles (FIPPs) rooted in the Privacy Act, and is well acquainted with the protection of American civil liberties

and privacy rights. This capability is a key reason why DHS should be a primary point of contact for coordinating cybersecurity and the protection of the Nation's critical infrastructure.

HEARINGS

On February 13, 2013, the Full Committee held a hearing entitled "A New Perspective on Threats to the Homeland." The Committee received testimony from ADM Thad Allen (Ret. USCG), Senior Vice President, Booz Allen Hamilton; Mr. Shawn Henry, President, CrowdStrike Services; Hon. Michael E. Leiter, Private Citizen; Hon. David M. Walker, Founder and CEO, The Comeback America Initiative; and Mr. Clark Kent Ervin, Partner, Patton Boggs, LLP.

On March 13, 2013, the Full Committee held a hearing entitled "DHS Cybersecurity: Roles and Responsibilities to Protect the Nation's Critical Infrastructure." The Committee received testimony from Hon. Jane Holl Lute, Deputy Secretary, U.S. Department of Homeland Security; Mr. Anish B. Bhimani, Chairman, Financial Services Information Sharing and Analysis Center; Mr. Gary W. Hayes, Chief Information Officer, Centerpoint Energy; and Ms. Michelle Richardson, Legislative Counsel, American Civil Liberties Union.

On March 20, 2013, the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies held a hearing entitled "Cyber Threats from China, Russia and Iran: Protecting American Critical Infrastructure." The Subcommittee received testimony from Mr. Frank J. Cilluffo, Director, Homeland Security Policy Institute and Co-Director, Cyber Center for National and Economic Security, The George Washington University; Mr. Richard Bejtlich, Chief Security Officer and Security Services Architect, Mandiant; Mr. Ilan Berman, Vice President, American Foreign Policy Council; and Mr. Martin C. Libicki, Senior Management Scientist, RAND Corporation.

On April 25, 2013, the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies held a hearing entitled "Striking the Right Balance: Protecting Our Nation's Critical Infrastructure from Cyber Attack and Ensuring Privacy and Civil Liberties." The Subcommittee received testimony from Ms. Mary Ellen Callahan, Partner, Jenner & Block and Former Chief Privacy Officer, U.S. Department of Homeland Security; Ms. Cheri F. McGuire, Vice President, Global Government Affairs and Cybersecurity Policy, Symantec; and Ms. Harriet Pearson, Partner, Hogan Lovells.

On May 16, 2013, the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies held a hearing entitled "Facilitating Cyber Threat Information Sharing and Partnering with the Private Sector to Protect Critical Infrastructure: An Assessment of DHS Capabilities." The Subcommittee received testimony from Ms. Roberta Stempfley, Acting Assistant Secretary, Office of Cybersecurity and Communications, U.S. Department of Homeland Security; Mr. Larry Zelvin, Director, National Cybersecurity and Communications Integration Center, U.S. Department of Homeland Security; and Mr. Charles K. Edwards, Acting Inspector General, U.S. Department of Homeland Security.

On July 17, 2013, the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies and the Committee on Oversight and Government Reform's Subcommittee on Energy Policy, Health Care and Entitlements held a joint hearing entitled "Evaluating Privacy, Security, and Fraud Concerns with ObamaCare's Information Sharing Apparatus." The Subcommittees received testimony from Mr. Alan R. Duncan, Assistant Inspector General for Security and Information Technology Services, Inspector General for Tax Administration, Department of the Treasury; Mr. Terence V. Milholland, Chief Technology Officer, Internal Revenue Service; Hon. Danny Werfel, Principal Deputy Commissioner, Internal Revenue Service; Hon. Marilyn B. Tavenner, Administrator, Centers for Medicare and Medicaid Services, U.S. Department of Health and Human Services; Mr. Henry Chao, Deputy Chief Information Officer, Deputy Director of the Office of Information Services, Centers for Medicare and Medicaid Services, U.S. Department of Health and Human Services; and Mr. John Dicken, Director, Health Care, U.S. Government Accountability Office.

On July 18, 2013, the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies held a hearing entitled "Oversight of Executive Order 13636 and Development of the Cybersecurity Framework." The Subcommittee received testimony from Mr. Robert Kolasky, Director, Implementation Task Force, National Protection and Programs Directorate, U.S. Department of Homeland Security; Charles H. Romine, PhD, Director, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce; and Eric A. Fischer, PhD, Senior Specialist, Science and Technology, Congressional Research Service, Library of Congress.

On September 11, 2013, the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies held a hearing entitled "The Threat to Americans' Personal Information: A Look into the Security and Reliability of the Health Exchange Data Hub." The Subcommittee received testimony from Mr. Michael Astrue, Former Social Security Commissioner, Former U.S. Department of Health and Human Services General Counsel; Stephen T. Parente, Ph.D., Minnesota Insurance Industry Chair of Health Finance, Director, Medical Industry Leadership Institute and Professor, Department of Finance, Carlson School of Management, University of Minnesota; Ms. Kay Daly, Assistant Inspector General, Audit Services, U.S. Department of Health and Human Services; and Mr. Matt Salo, Executive Director, National Association of Medicaid Directors.

On November 13, 2013, the Full Committee held a hearing entitled "Cyber Side-Effects: How Secure is the Personal Information Entered into the Flawed Healthcare.gov?" The Committee received testimony from Ms. Roberta "Bobbie" Stempfley, Acting Assistant Secretary, Office of Cybersecurity and Communications, U.S. Department of Homeland Security; Ms. Soraya Correa, Associate Director, Enterprise Services Directorate, U.S. Citizenship and Immigration Services, U.S. Department of Homeland Security; Mr. Luke Chung, President, FMS, Inc.; and Mr. Waylon Krush, Chief Executive Officer, Lunarline, Inc.

COMMITTEE CONSIDERATION

The Committee met on February 5, 2014, to consider H.R. 3696, and ordered the measure to be reported to the House with a favorable recommendation, amended, by voice vote. The Committee took the following actions:

The Committee adopted H.R. 3696, as amended, by voice vote.

The following amendments were offered:

An Amendment in the Nature of a Substitute offered by MR. McCAUL (#1); was AGREED TO by voice vote.

An amendment to the Amendment in the Nature of a Substitute to H.R. 3696 offered by MS. LORETTA SANCHEZ OF CALIFORNIA (#1A); further discussion on the amendment was POSPONED.

Page 12, line 6, strike “and”.

Page 12, line 11, strike the period and insert “; and”.

Page 12, beginning line 12, insert a new subparagraph (F).

A modified version of an amendment to the Amendment in the Nature of a Substitute to H.R. 3696 offered by MS. LORETTA SANCHEZ OF CALIFORNIA (#1A); was WITHDRAWN by unanimous consent.

Page 12, line 6, strike “and”.

Page 12, line 11, strike the period and insert “; and”.

Page 12, beginning line 12, insert a new subparagraph (F).

An en bloc amendment to the Amendment in the Nature of a Substitute to H.R. 3696 offered by MRS. BROOKS (#1B); was AGREED TO by voice vote.

An amendment:

Page 31, line 19, strike “and”.

Page 32, line 16, strike the period and insert “; and”.

Page 32, beginning line 17, insert the following: “(12) participate in exercises run by the Department’s National Exercise Program, where appropriate;”

An amendment:

Page 32, line 18, insert “, in coordination with the Office of Intelligence and Analysis of the Department,” before “shall maintain”;

An amendment:

Page 33, line 16, strike “and”.

Page 33, line 20, strike the period and insert “;and”.

Page 33, beginning line 21, insert the following:

“(5) assess and evaluate consequence, vulnerability, and threat information regarding cyber incidents in coordination with the Office of Emergency Communications of the Department to help facilitate continuous improvements to the security and resiliency of public safety communications networks.

An amendment:

Page 37, line 24, strike the close quotes and the second period.

Page 38, beginning line 1, insert a new subsection entitled ‘(d) Update to Cyber Incident Annex to the National Response Framework.’

An en bloc amendment to the Amendment in the Nature of a Substitute to H.R. 3696 offered by MS. JACKSON LEE (#1C); was AGREED TO by voice vote.

An amendment:

Page 30, line 3, insert the following (and redesignate subsequent paragraphs accordingly):

“(5) collaborate and facilitate discussions with Sector Coordinating Councils, Information Sharing and Analysis Centers, Sector Specific Agencies, and relevant critical infrastructure sectors on the development of prioritized response efforts, if necessary, to support the defense and recovery of critical infrastructure from cyber incidents;

An amendment:

Page 12, line 6, strike “and”.

Page 12, line 11, strike the period and insert “; and”.

Page 12, beginning line 12, insert the following:

“(F) conduct outreach to educational institutions, including historically black colleges and universities, Hispanic serving institutions, Native American colleges, and institutions serving persons with disabilities, to encourage such institutions to promote cybersecurity awareness.

An amendment:

Page 37, line 19, strike “and”.

Page 37, line 24, strike the close quotes and the first and second periods and insert “; and”.

Page 38, beginning line 1, insert a new paragraph (3).

An amendment:

Page 41, beginning line 1, insert a new subsection entitled “(e) Resources Information.”

An amendment:

Page 53, beginning line 3, insert a new section (and conform the table of contents accordingly): entitled “Sec. 206. Cybersecurity Scholars.”

An amendment to the Amendment in the Nature of a Substitute to H.R. 3696 offered by MR. BARBER (#1D); was AGREED TO by voice vote.

Page 11, line 3, insert “using a risk-based and performance-based approach” after “Federal civilian information systems”.

An amendment to the Amendment in the Nature of a Substitute to H.R. 3696 offered by MR. PAYNE (#1E); was AGREED TO by voice vote,

Page 53, beginning line 3, insert a new section entitled “Sec. 206. National Research Council Study on the Resilience and Reliability of the Nation’s Power Grid.”

An amendment to the Amendment in the Nature of a Substitute to H.R. 3696 offered by MR. SWALWELL (#1F); was AGREED TO by voice vote.

Page 9, line 12, insert “national laboratories,” before “critical infrastructure owners”.

An amendment to the Amendment in the Nature of a Substitute to H.R. 3696 offered by MR. SWALWELL (#1G); was WITHDRAWN by unanimous consent,

Page 49, line 18, insert “, and, unless otherwise prohibited by law, with respect to which the Secretary publishes in the Federal Register an explanation therefor,” after “determines”.

The Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies met on January 15, 2014, to consider H.R. 3696, and ordered the measure reported to the Full Committee with a favorable recommendation, amended, by voice vote. The Subcommittee took the following actions:

The Subcommittee agreed to H.R. 3696, as amended, by voice vote.

The following amendments were offered:

An Amendment by MR. MEEHAN (#1); was AGREED TO by voice vote.

Page 3, line 2, strike “resulting in”.

In section 101, in the proposed amendment to section of the Homeland Security Act of 2002, strike the proposed paragraphs (23), (25), and (32), and redesignate the proposed paragraphs (24), (26), (27), (28), (29), (30), (31), and (33) as paragraphs (23) through (30), respectively.

Page 11, beginning line 24, strike “upon request, facilitate and assist risk management efforts of entities” and insert “upon request of entities, facilitate and assist risk management efforts of such entities”.

Page 12, beginning line 4, strike “‘upon request, provide education and assistance to critical infrastructure owners and critical infrastructure operators’” and insert “‘upon request of critical infrastructure owners or critical infrastructure operators, provide education and assistance to such owners and operators’”.

Page 12, beginning line 18, strike “‘upon request, support critical infrastructure owners’ and critical infrastructure operators’ efforts’” and insert “‘upon request of critical infrastructure owners or critical infrastructure operators, support such owners’ and operators’ efforts’”.

Page 13, line 5, insert “‘build upon existing mechanisms to’” before “‘promote’”.

Page 13, line 8, strike “‘upon request,’” and insert “‘upon request of Federal, State, and local government entities and private entities,’”.

Page 16, line 1, insert “‘and partner with’” before “‘the Sector Coordinating Council’”.

Page 17, beginning line 1, insert a new paragraph entitled “(C) Limitation.—”

Page 22, strike lines 1 through 5 and insert a new subsection entitled “(f) Clearances.—”

Page 22, line 21, insert “‘and implement’” after “‘develop’”.

Page 27, line 3, strike “‘(i)’” and insert “‘(j)’”.

Page 27, beginning line 3, insert a new subsection entitled “(i) Recommendations Regarding New Agreements.”

Page 44, lines 17 and 22, strike “‘collaboration’” and insert “‘coordination’” each place it appears.

Page 48, beginning line 13, strike “‘or business-sensitive information’” and insert “‘, business-sensitive information, or other sensitive information’”.

Page 54, line 6, insert “(except that this section shall not apply in the case of section 202 of this Act and the amendments made by such section 202)” before “do”.

An en bloc Amendment by MS. CLARKE (#2); was AGREED TO by voice vote.

An amendment: Add at the end a new title entitled “Title III—Homeland Security Cybersecurity Boots-on-the-Ground.”

An amendment: Page 53, line 25, strike “the Science and Technology Directorate of”.

An Amendment by MR. ROGERS OF ALABAMA (#3); was WITHDRAWN by unanimous consent.

Page 53, line 19, strike “‘severely’”.

An Amendment by MR. HORSFORD (#4); was AGREED TO by voice vote.

Page 43, beginning line 10, strike “elevate” and insert “protect and maintain operations in accordance with the Office’s mission to provide incentives for the development and deployment of anti-terrorism technologies while elevating”.

An Amendment by MR. DAINES (#5); was AGREED TO by voice vote.

Page 32, line 3, strike “‘and’”.

Page 32, line 7, strike the period at the end and insert “‘; and’”.

Page 32, beginning line 8, insert a new paragraph (11).

Page 33, line 19, insert “‘the extent of any personally identifiable information that was involved,’ ” after “‘breaches,’”.

An Amendment by MR. PERRY (#6); was AGREED TO by voice vote.

Add at the end of title II a new section entitled “Sec. 205. Prohibition on the Collection of Personally Identifiable Information for Cybersecurity Purposes.”

COMMITTEE VOTES

Clause 3(b) of Rule XIII of the Rules of the House of Representatives requires the Committee to list the recorded votes on the motion to report legislation and amendments thereto.

No recorded votes were requested during consideration of H.R. 3696.

COMMITTEE OVERSIGHT FINDINGS

Pursuant to clause 3(c)(1) of Rule XIII of the Rules of the House of Representatives, the Committee has held oversight hearings and made findings that are reflected in this report.

NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

In compliance with clause 3(c)(2) of Rule XIII of the Rules of the House of Representatives, the Committee finds that H.R. 3696, the National Cybersecurity and Critical Infrastructure Protection Act of 2013, would result in no new or increased budget authority, entitlement authority, or tax expenditures or revenues.

CONGRESSIONAL BUDGET OFFICE ESTIMATE

The Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, April 30, 2014.

Hon. MICHAEL MCCAUL,
*Chairman, Committee on Homeland Security,
House of Representatives, Washington, DC.*

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate H.R. 3696, the National Cybersecurity and Critical Infrastructure Protection Act of 2014.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Jason Wheelock.

Sincerely,

DOUGLAS W. ELMENDORF.

Enclosure.

H.R. 3696—National Cybersecurity and Critical Infrastructure Protection Act of 2014

Summary: H.R. 3696 would amend the Homeland Security Act of 2002 to require the Secretary of the Department of Homeland Security (DHS) to conduct cybersecurity activities on behalf of the federal government and would codify the role of DHS in preventing and responding to cybersecurity incidents involving the Information Technology (IT) systems of federal civilian agencies and critical infrastructure in the United States.

Although DHS currently conducts many of the activities covered by H.R. 3696 and has received approximately \$800 million so far in fiscal year 2014 for its cybersecurity activities, some provisions in the bill would expand existing programs, provide additional authorities, or add new requirements beyond the agency's current efforts. Assuming the appropriation of the necessary amounts, CBO estimates that implementing the bill would cost an additional \$160 million over the 2015–2019 period.

Pay-as-you-go procedures do not apply to this legislation because it would not affect direct spending or revenues.

H.R. 3696 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA).

Estimated cost to the Federal Government: The estimated budgetary impact of H.R. 3696 is shown in the following table. The costs of this legislation fall within budget function 050 (national defense).

	By fiscal year, in millions of dollars—					
	2015	2016	2017	2018	2019	2015–2019
CHANGES IN SPENDING SUBJECT TO APPROPRIATION						
Funding for Information Sharing and Analysis Centers						
Estimated Authorization Level	25	25	0	0	0	50
Estimated Outlays	9	18	16	7	0	50
DHS Cybersecurity Personnel and Authorities						
Estimated Authorization Level	0	26	25	26	30	106
Estimated Outlays	0	23	25	26	30	104
Information Technology Scholarships						
Estimated Authorization Level	*	1	1	1	1	4
Estimated Outlays	*	1	1	1	1	4
Homeland Security Cybersecurity Boots on the Ground Act						
Estimated Authorization Level	*	*	*	*	*	2
Estimated Outlays	*	*	*	*	*	2
Total Changes.						
Estimated Authorization Level	25	50	26	27	31	162
Estimated Outlays	9	42	42	34	31	160

Note: Numbers may not sum to totals because of rounding; DHS = Department of Homeland Security; * = less than \$500,000.

Basis of estimate: For this estimate, CBO assumes that the bill will be enacted near the beginning of fiscal year 2015 and that spending will follow historical patterns for similar activities.

Funding for Information Sharing and Analysis Centers

Section 103 would require that at least \$25 million of the funds provided to DHS's Office of Cybersecurity and Communications in fiscal years 2014 to 2016 be used to support the presence of Information Sharing Analysis Centers (ISAC) at DHS's National Cybersecurity and Communications Integration Center (NCCIC). ISACs are private centers that serve as conduits for passing cybersecurity and other information between DHS and private organizations. They are also responsible for coordinating the response of the private sector and the federal government to cybersecurity incidents and other events affecting the nation's critical infrastructure. At present, there is no dedicated funding provided to support the operations of such centers at the NCCIC and amounts spent for such purposes are insignificant.

H.R. 3696 also would require that DHS recognize at least one ISAC for each of the 16 critical infrastructure sectors listed in the bill. Because we assume that H.R. 3696 will be enacted near the beginning of fiscal year 2015, CBO estimates that implementing this provision would have no cost in 2014, but would cost \$50 million over the 2015–2018 period, assuming that appropriations of \$25 million are provided for such purposes in 2015 and 2016.

DHS Cybersecurity Personnel Authorities

Section 302 would provide DHS with enhanced authorities for hiring and compensating DHS employees who perform cybersecurity functions in support of federal civilian agencies and critical infrastructure. Under those authorities, DHS could convert eligible

positions to the excepted service and would have expanded flexibility in determining pay and bonuses for employees in those positions. (Excepted service authorities allow for expediting the hiring of individuals into federal service by allowing agencies to fill positions without following the procedures, rules, and classifications required for hiring employees into the competitive service.)

The Transportation Security Administration (TSA) has hiring and pay authorities similar to those that would be provided under section 302. CBO analysed data from the Office of Personnel Management for TSA employees in the field of information technology management and found that, after accounting for years of service and education, employees in that category earned about 15 percent more at TSA than elsewhere at DHS. On that basis, CBO anticipates that pay for positions established in the excepted service under this proposal would increase by about 15 percent above current levels.

According to DHS, approximately 1,500 employees, mostly in grades GS-13, GS-14, and GS-15, would be transitioned into a new pay plan for cybersecurity specialists under this provision. However, CBO estimates that 100 of those individuals are in TSA, and would not see a pay increase under the plan. For the remaining 1,400 employees, based on the difference in pay and the number and grades of the employees to be transitioned, CBO estimates that implementing this provision would cost \$104 million over the 2016–2019 period, assuming the appropriation of the necessary amounts.

Information Technology Scholarships

Section 302 also would authorize DHS to establish a scholarship program similar to the Information Assurance Scholarship Program (IASP) of the Department of Defense (DoD).

The IASP is designed to assist DoD in recruiting and retaining IT personnel in the field of information assurance. The program currently has about 100 participants, and awards scholarships and stipends to both undergraduate and graduate students. Based on information about the size and cost of the DoD program, CBO estimates that DHS would provide scholarships and stipends to about 20 people a year at a cost of \$4 million over the 2015–2019 period, assuming appropriation of the necessary amounts.

Homeland Security Cybersecurity Boots on the Ground Act

Section 301 would require DHS to maintain documentation verifying that contractors who serve in cybersecurity roles at DHS have received the training necessary to perform their assigned responsibilities. CBO anticipates that effort would require additional staffing and resources. Based on the cost of similar personnel, CBO estimates that implementing that requirement would cost approximately \$2 million over the 2015–2019 period, subject to the availability of appropriated funds.

Pay-As-You-Go considerations: None.

Intergovernmental and private-sector impact: H.R. 3696 contains no intergovernmental or private-sector mandates as defined in UMRA.

Estimate prepared by: Federal Costs: Jason Wheelock; Impact on state, local, and tribal governments: Melissa Merrell; Impact on the private sector: Elizabeth Bass.

Estimate approved by: Theresa Gullo, Deputy Assistant Director for Budget Analysis.

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of Rule XIII of the Rules of the House of Representatives, H.R. 3696 contains the following general performance goals and objectives, including outcome related goals and objectives authorized.

H.R. 3696 will strengthen the National Cybersecurity and Communications Integration Center (NCCIC), a Federal civilian, transparent interface to facilitate real-time cyber threat information sharing across critical infrastructure sectors. In furtherance of fostering an effective partnership between private industry and the Department, H.R. 3696 directs DHS to leverage industry-led organizations to facilitate critical infrastructure protection and incident response, as appropriate. H.R. 3696 also seeks to enable the Department to provide timely technical assistance, crisis management, and actionable recommendations on cyber threats to critical infrastructure owners and operators on a voluntary basis, will ensure that a National Cybersecurity Incident Response Plan is developed and exercised, and will clarify DHS' operational information security activities to protect and ensure the integrity and resiliency of all Federal civilian information systems and networks operating in the ".gov" domain. H.R. 3696 will also clarify that cybersecurity technologies and services may be certified by the DHS SAFETY Act Office so private entities can voluntarily submit their cybersecurity procedures to the SAFETY Act Office. Additionally, H.R. 3696 establishes another liability protection threshold in the event of a "qualifying cyber incident" under the SAFETY Act.

Finally, H.R. 3696 recognizes that for DHS to fulfill its cybersecurity responsibilities, it needs to recruit, develop, and retain a cadre of professionals with cyber skills. To that end, H.R. 3696 requires DHS to develop a comprehensive workforce assessment and strategy to address gaps in the Nation's cybersecurity workforce. Additionally, it provides special hiring authority to ensure that the Department can compete with other Federal and private sector employers for talented cyber professionals.

CONGRESSIONAL EARMARKS, LIMITED TAX BENEFITS, AND LIMITED TARIFF BENEFITS

In compliance with Rule XXI of the Rules of the House of Representatives, this bill, as reported, contains no congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(e), 9(f), or 9(g) of the Rule XXI.

FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

PREEMPTION CLARIFICATION

In compliance with section 423 of the Congressional Budget Act of 1974, requiring the report of any Committee on a bill or joint resolution to include a statement on the extent to which the bill or joint resolution is intended to preempt State, local, or Tribal law, the Committee finds that H.R. 3696 does not preempt any State, local, or Tribal law.

ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short Title.

This section provides that bill may be cited as the “National Cybersecurity and Critical Infrastructure Protection Act of 2014” or the “NCCIP Act”.

Sec. 2. Table of Contents.

This section details the contents of this legislation.

TITLE I—SECURING THE NATION AGAINST CYBER ATTACK

Sec. 101. Homeland Security Act of 2002 definitions.

This section defines certain terminology used in this legislation, including definitions for “critical infrastructure”, “critical infrastructure owner”, “critical infrastructure operator”, “cyber incident”, “cybersecurity mission”, “cybersecurity purpose”, “cyber threat”, “cyber threat information”, “Federal civilian information systems”, “information security”, “information system”, “private entity”, and “shared situational awareness”.

Sec. 102. Enhancement of cybersecurity.

This section requires the Secretary of Homeland Security, in collaboration with other appropriate Federal Government entities, to conduct cybersecurity activities to provide shared situational awareness and enable real-time, integrated, and operational actions to protect from, prevent, mitigate, respond to, and recover from cyber incidents.

The Federal Government continues to make progress building up the Nation’s cybersecurity capabilities and increasing collaboration across the various Federal agencies that have responsibility for cybersecurity matters. Over the past several years, this interagency collaboration has evolved, solidifying the U.S. Federal Cybersecurity Operations Team in three Federal departments—the Department of Homeland Security (DHS), the Department of Justice (DOJ), and the Department of Defense (DoD). Executive Order 13636, Improving Critical Infrastructure Cybersecurity, issued Feb-

bruary 2013, states that “. . . the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence shall each issue instructions consistent with their authorities . . . to ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity.” The U.S. Federal Cybersecurity Operations Team takes a whole-of-government and collaborative approach to increasing coordination across Federal agencies and is meant to ensure the Nation’s cybersecurity capabilities are effective, agile, and responsive to the evolving cybersecurity threat to the United States. In order to properly function and meet the cybersecurity mission needs of the Federal Government, this capability must allow for shared situational awareness that enables real-time and integrated operational actions under each department’s respective authorities. Broadly, the National roles and responsibilities for cybersecurity are as follows:

- The Department of Homeland Security—Lead for Protection;
- The Department of Justice—Lead for Investigation; and
- The Department of Defense—Lead for National Defense.

The Committee expects the National Cybersecurity and Communications Integration Center (NCCIC) within the Department of Homeland Security to be the Federal civilian entity that collaborates with the U.S. Federal Cybersecurity Operations Team and provides shared situational awareness to the Department of Justice and the Department of Defense to enable real-time, integrated, and operational actions to protect from, prevent, mitigate, respond to, and recover from cyber incidents.

Executive Order 13636, Section 4, states that “the Secretary [of Homeland Security] and the Attorney General, in coordination with the Director of National Intelligence, shall establish a process that rapidly disseminates the reports produced . . . to the targeted entity.” Further, “the Secretary [of Homeland Security] and the Attorney General, in coordination with the Director of National Intelligence, shall establish a system for tracking the production, dissemination, and disposition of these reports.”

SUBTITLE C—CYBERSECURITY AND INFORMATION SHARING

Sec. 103. Protection of critical infrastructure and information sharing.

(a) Protection of Critical Infrastructure

This subsection requires the Secretary of Homeland Security to coordinate, on an ongoing basis, with Federal, State, and local governments, National Laboratories, critical infrastructure owners, critical infrastructure operators, and other cross sector coordinating entities to: (1) Facilitate a national effort to strengthen and maintain secure and resilient critical infrastructure; (2) ensure DHS policies and procedures enable real-time, actionable, and relevant cyber threat information sharing; (3) seek industry sector-specific expertise; (4) reduce vulnerabilities, identify and disrupt threats, minimize consequences, and provide education and assistance to critical infrastructure owners and operators to strengthen the security and resiliency of the Nation’s critical infrastructure; and (5) co-

ordinate a research and development strategy to promote advancements and innovation in cybersecurity technologies.

Additionally, the Secretary is directed to manage Federal efforts to secure, protect, and ensure the resiliency of Federal civilian information systems, and promote a national awareness effort to educate the general public on the importance of securing information systems.

The Committee expects the Secretary to direct the National Cybersecurity and Communications Integration Center within the Department to act as a Federal civilian entity to provide multi-directional sharing of real-time, actionable, and relevant cyber threat information. Finally, the Secretary is directed to facilitate cyber incident response and recovery assistance and engage international and educational partners to promote cybersecurity awareness and strengthen the security and resiliency of critical infrastructure.

Nothing in this section requires any private entity to request assistance from the Secretary, nor does it require any private entity requesting assistance to implement any measure or recommendation suggested by the Secretary.

The Nation's critical infrastructure provides the vital services that fuel the U.S. economy, ensures public health and safety, and preserves American culture and way of life. Today, critical infrastructure owners and operators are increasingly leveraging information technology (IT) systems and connecting to the Internet to increase their efficiency and productivity. While such technological advancements offers many benefits, cyberspace is also a highly interconnected and complex domain with inherent vulnerabilities that when compromised could be both disruptive and destructive to critical information systems. Adding to the complexity, an increasingly interconnected society with interdependent and distributed information systems transcends across sectors and could cause cascading and consequential impacts to other critical infrastructure sectors. The Committee agrees with the provision in Executive Order 13636 that states, "It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties."

Within the private sector, individual corporations and business entities are responsible for securing their own IT systems. Most critical infrastructure within the U.S. is owned and operated by private entities, so the security of this critical infrastructure is ultimately the responsibility of those private entities. That said, many sectors of critical infrastructure (*e.g.* energy, financial) are already regulated by the U.S. government and are subject to security oversight, both physical security and cybersecurity. While a good number of private entities and critical infrastructure owners and operators have already made significant investments and efforts in managing their own cybersecurity risks and vulnerabilities, many other entities, including many small and medium sized businesses, have limited resources or are just now beginning to understand the growing cybersecurity risks they face.

Today, criminals, hacktivists, terrorists, and nation-state actors, such as Russia, China and Iran, increasingly use sophisticated malware and take relentless efforts to disrupt or destroy U.S. crit-

ical infrastructure, which has left many of these entities to defend against these threats themselves. According to Executive Order 13636, “repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront.”

With our Nation’s critical infrastructure so vital to our National security, economic stability and public safety, greater collaboration and a national unity of effort is needed between the public and private sector and across all sectors to strengthen and maintain secure, functioning, and resilient critical infrastructure from cyber threats. The Committee believes that providing public education and voluntary assistance to private entities can help business owners and operators of critical infrastructure to more effectively manage their cybersecurity risk. Recognizing the importance of sharing security best practices and cyber threat information, the Department of Homeland Security continues to facilitate such communications among and between each of these critical infrastructure sectors.

(b) Critical Infrastructure Sectors

This section requires the Secretary to designate critical infrastructure sectors, which may change, or include subdivisions within sectors as needs arise.

Title II of the Homeland Security Act of 2002 (Pub. L. 107–296) sets forth the Department of Homeland Security’s responsibilities for critical infrastructure protection. For the last decade, the Homeland Security Presidential Directive 7 (HSPD–7), issued December 17, 2003, established the national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks. HSPD–7 states “In carrying out the functions assigned in the Homeland Security Act of 2002, the Secretary shall be responsible for coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States. The Secretary shall serve as the principal Federal official to lead, integrate, and coordinate implementation of efforts among Federal departments and agencies, State and local governments, and the private sector to protect critical infrastructure and key resources.”

In February 2013, the Administration issued Presidential Policy Directive-21 (PPD–21), which replaced HSPD–7. As in HSPD–7, PPD–21 provides, “the Secretary of Homeland Security shall provide strategic guidance, promote a national unity of effort, and coordinate the overall Federal effort to promote the security and resilience of the Nation’s critical infrastructure. In carrying out the responsibilities assigned in the Homeland Security Act of 2002, as amended, the Secretary of Homeland Security evaluates national capabilities, opportunities, and challenges in protecting critical infrastructure; analyzes threats to, vulnerabilities of, and potential consequences from all hazards on critical infrastructure; identifies security and resilience functions that are necessary for effective public-private engagement with all critical infrastructure sectors; develops a national plan and metrics, in coordination with (Sector Specific Agencies) SSAs and other critical infrastructure partners; integrates and coordinates Federal cross-sector security and resil-

ience activities; identifies and analyzes key interdependencies among critical infrastructure sectors; and reports on the effectiveness of national efforts to strengthen the Nation's security and resilience posture for critical infrastructure."

In accordance with the Homeland Security Act of 2002, and pursuant to the requirements set forth by the President in HSPD-7 and PPD-21, in 2006, and subsequently in 2009 and 2013, the Department of Homeland Security in its role as coordinator for infrastructure protection issued the National Infrastructure Protection Plan (NIPP). The 2013 version of the NIPP is based on the evolution and maturation of the public-private partnership framework to facilitate a national effort in protecting U.S. critical infrastructure. It provides an integrated and collaborative approach of our national effort to share threat information, manage risks, reduce vulnerabilities, minimize consequences, and respond and recover from incidents affecting critical infrastructure. According to the Government Accountability Office, "the NIPP is intended to provide the framework for a coordinated national approach to address the full range of physical, cyber, and human threats and vulnerabilities that pose risks to the nation's critical infrastructure. The NIPP relies on a sector partnership platform as the primary means of coordinating government and private sector critical infrastructure protection efforts. Under this model, each sector has both a government council and a private sector council to address sector-specific planning and coordination." The Committee expects that the NIPP framework, which has been supported by the private sector since its inception, will continue to be the public-private partnership model that governs our efforts in protecting the Nation's critical infrastructure from a cyber attack.

PPD-21 and the updated NIPP organizes critical infrastructure into 16 critical infrastructure sectors with the Secretary of Homeland Security periodically evaluating the need for and approving changes to critical infrastructure sectors. The Committee expects that critical infrastructure sectors will change overtime due to technological advancements and a changing economy. The critical infrastructure sectors are the following:

1. Food and Agriculture
2. Financial Services
3. Chemical
4. Commercial Facilities
5. Communications
6. Critical Manufacturing
7. Dams
8. Defense Industrial Base
9. Emergency Services
10. Energy
11. Government Facilities
12. Healthcare and Public Health
13. Information Technology
14. Nuclear Reactors, Materials and Waste
15. Transportation Systems
16. Water and Wastewater Systems

(c) *Sector Specific Agencies*

This subsection requires the Secretary, in collaboration with the relevant critical infrastructure sector and the heads of other appro-

priate Federal agencies, to recognize the Federal agency designated as of November 1, 2013, as the “Sector-Specific Agency” for each critical infrastructure sector. There are 16 different critical infrastructure sectors that each has a designated Sector Specific Agency (SSA). Each SSA is responsible for collaborating with private sector partners and encouraging voluntary information sharing and analysis within each sector. The designated agency will support the security and resiliency activities of the sector and provide institutional knowledge and specialized expertise to relevant critical infrastructure sectors.

The Committee expects that this policy will be carried out in accordance with PPD–21 which states, “Recognizing existing statutory or regulatory authorities of specific Federal departments and agencies, and leveraging existing sector familiarity and relations, Sector Specific Agencies shall carry out the following roles and responsibilities for their respective sectors: 1) As part of the broader national effort to strengthen the security and resilience of critical infrastructure, coordinate with the Department of Homeland Security (DHS) and other relevant Federal departments and agencies, and collaborate with critical infrastructure owners and operators

.”
H.R. 3696 does not alter or modify the current relationships between existing critical infrastructure sectors and their respective Sector-Specific Agencies. The following designated Sector-Specific Agencies for each critical infrastructure sector are the following:

T4Critical Infrastructure Sector

CRITICAL INFRASTRUCTURE SECTOR	SECTOR SPECIFIC AGENCY
Food and Agriculture	Department of Agriculture Department of Health and Human Services
Financial Services	Department of the Treasury
Chemical	Department of Homeland Security
Commercial Facilities	Department of Homeland Security
Communications	Department of Homeland Security
Critical Manufacturing	Department of Homeland Security
Dams	Department of Homeland Security
Defense Industrial Base	Department of Defense
Emergency Services	Department of Homeland Security
Energy	Department of Energy
Government Facilities	Department of Homeland Security General Services Administration
Healthcare and Public Health Services ...	Department of Health and Human Services
Information Technology	Department of Homeland Security
Nuclear Reactors, Materials, and Waste	Department of Homeland Security
Transportation Systems	Department of Homeland Security
Water and Wastewater Systems	Environmental Protection Agency

(d) Sector Coordinating Councils

This subsection directs the Secretary, in collaboration with each critical infrastructure sector and the relevant Sector Specific Agen-

cy, to recognize and partner with the Sector Coordinating Council (SCC) for each critical infrastructure sector. The recognized Sector Coordinating Councils will serve as the primary industry-led policy, planning, and communications entities for coordination with the Department, the relevant Sector-Specific Agencies, and relevant Information Sharing and Analysis Centers, and will be comprised of relevant small, medium, and large critical infrastructure owners and operators, private entities, and representative trade associations. The Secretary has no role in the determination of membership of any Sector Coordinating Council. The Committee expects each Sector Coordinating Council to establish its own governance and operating procedures to coordinate with the Department and any relevant Information Sharing Analysis Centers, and identify gaps concerning infrastructure protection to help inform research and development.

Each critical infrastructure sector has a Sector Coordinating Council to serve as an organizational entity to more effectively coordinate cybersecurity activities amongst the sector, the Department of Homeland Security, and with each relevant Sector Specific Agency. The Committee believes that in order to have a productive and collaborative public-private partnership all parties need clarity about the terms of the partnership and each should have a clear understanding of each other's roles and responsibilities. In the event of a cyber attack, ambiguity in respective roles and responsibilities could delay and obstruct a coordinated response and the ability to quickly respond and recover from a cyber incident.

(e) Sector Information Sharing and Analysis Centers

This subsection requires the Secretary, in collaboration with the relevant Sector Coordinating Council (SCC) and the critical infrastructure sector represented by the Council and in coordination with the relevant Sector Specific Agency, to recognize at least one official Information Sharing and Analysis Center (ISAC) for each critical infrastructure sector. The Committee does not expect this subsection to preclude any other ISAC from having an information sharing relationship with the NCCIC. The ISACs will serve as an information sharing resource for each sector and promote on-going multi-directional sharing of real-time, relevant, and actionable cyber threat information and analysis by and among each sector, the Department, Sector-Specific Agencies, and other critical infrastructure ISACs. The ISACs serve as the primary private sector interface with the NCCIC.

This subsection reallocates funds, a minimum of \$25,000,000 per year for three years, from the Cybersecurity and Communications Office for operations support at the NCCIC for all recognized ISACs.

The concept of ISACs for each critical infrastructure sector was first developed in the late 1990's during the Clinton Administration and articulated in Presidential Decision Directive (PDD)-63. While some sectors such as Financial Services, Information Technology and Communications have more mature ISACs, other sectors have ISACs at varying levels of maturity ranging from fully functional to non-existent. The Committee expects that the most mature sector ISACs will serve as an operational model for other less mature sector ISACs. Additionally, the Committee believes that enhanced participation from all critical infrastructure ISACs would signifi-

cantly increase the quality and quantity of multi-directional information sharing between the public and private sector.

Today, there are a limited amount of critical infrastructure sectors that are permanent residents on the floor of the NCCIC. The Committee staff has heard from many ISACs who wish to have a presence on the NCCIC floor but do not have the funding or mechanisms in place to do so. The Committee believes there is significant value having all critical infrastructure sectors represented on the NCCIC floor. This would not only increase real-time information sharing and threat analysis, but also help foster stronger partnerships across all 16 critical infrastructure sectors. Accordingly, the bill provides an allocation of funding to support recognized ISACs at the NCCIC. It should be noted that similar funding was provided to several ISACs at the early stages of their creation.

(f) Clearances

This subsection requires the Secretary to expedite the security clearance process for appropriate members of the Sector Coordinating Councils, the ISACs, as well as any appropriate critical infrastructure owners and operators and any other person determined by the Secretary.

The Secretary of Homeland Security, as the Executive Agent for the Classified National Security Information Program established under Executive Order 13549 of August 18, 2010, shall expedite the processing of security clearances to appropriate personnel employed by critical infrastructure owners and operators.

The Committee has heard from many critical infrastructure owners and operators who are currently members of ISACs and SCCs and who have requested security clearances so that they can receive classified cybersecurity threat information. Unfortunately, these requests are not always processed in a timely fashion, thereby impeding the ability for need-to-know critical infrastructure owners and operators to receive such information and take the necessary action to defend their information systems from cyber threats. A cornerstone of this legislation is the public-private partnership between government and the private sector. Expediting security clearances will further build a more collaborative partnership in addressing cybersecurity threats to U.S. critical infrastructure.

(g) Public-Private Collaboration

This subsection requires the Secretary to collaborate with the Sector Specific Agencies, Sector Coordinating Councils, and critical infrastructure sectors to analyze and evaluate the current public-private partnership model and to ensure development and implementation of continuous and effective interactions among the parties. Critical infrastructure sectors are to have a reasonable period of time to review and comment on all jointly produced materials.

With the Department filling the role as coordinator, it is important that a functioning and mutually beneficial partnership be developed between the Federal Government and the various other sector specific agencies and the private sector owners and operators of critical infrastructure.

The public-private partnership remains a key part of the Nation's efforts to secure and protect its critical cyber-reliant infrastructure. If properly developed and implemented, the public-private partner-

ship model for cybersecurity can be leveraged to improve the culture of security and the willingness of the private sector partners to secure their critical infrastructure so vital to our country.

The partnership envisioned by the NIPP not only allows for, but depends upon, robust coordination and information sharing between the government and private sector owners and operators of critical infrastructure. The NIPP states, “Efficient information-sharing and information-protection processes based on mutually beneficial trusted relationships help ensure implementation of effective, coordinated, and integrated CIKR (critical infrastructure and key resources) protection programs and activities. Information sharing enables both government and private sector partners to assess events accurately, formulate risk assessments, and determine appropriate courses of action.”

Approximately 85 percent of the Nation’s critical infrastructure is owned by the private sector. Physical and cybersecurity of our Nation’s critical infrastructure must be carried out in a collaborative partnership between the government and the private sector. The Committee has received information and testimony that there was more of a constructive partnership between the government and the private sector back when the National Infrastructure Protection Plan was first established than there is today. This provision seeks to recalibrate the relationship as an effective partnership.

(h) Protection of Federal Civilian Information Systems

This subsection requires the Secretary to administer the operational information security activities and functions to protect and ensure the resiliency of all Federal civilian information systems. This subsection codifies the authorities given to the Department on July 6, 2010 in the Office of Management and Budget Memorandum M–10–28, “Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security.” It also codified the authorities given to the Department on January 8, 2008, in the National Security Presidential Directive (NSPD–54) and the Homeland Security Presidential Directive (HSPD–23). The Secretary will, in coordination with the heads of other Federal civilian agencies, develop issue and oversee the implementation and compliance of all operational information security policies; administer Federal Government-wide efforts to develop and provide adequate information security capabilities; establish and sustain continuous diagnostics to aggregate data and identify and prioritize the mitigation of cyber vulnerabilities; develop and operate intrusion capabilities to defend Federal civilian information systems from cyber threats; develop and conduct targeted risk assessments; develop and provide technical assistance; review operational information security activities annually; develop minimum technology neutral operational requirements; develop agency reporting requirements to the National Cybersecurity and Communications Integration Center (NCCIC); develop technology neutral performance requirements and metrics; implement training requirements that include industry recognized certifications; and develop training requirements regarding privacy, civil liberties oversight. This subsection authorizes the Secretary to enter into contracts or other agreements to carry out this subsection; however, no cause of action shall exist against private enti-

ties for assistance provided to the Secretary in accordance with this section.

On July 6, 2010, OMB issued Memorandum M-10-28 (the Memorandum) that bifurcated OMB and DHS' role in the protection of Federal civilian information systems. This was a result of OMB not having the capabilities nor having the resources to undertake the monumental task of facilitating the flow of breach information across the .gov domain. In fact, OMB currently only has the equivalent of two full-time employees responsible for managing the security of Federal civilian government information networks.

Pursuant to the Memorandum, DHS has primary responsibility within the executive branch for the operational aspects of Federal agency cybersecurity and is responsible for overseeing the protection of the .gov domain. Additionally, DHS is directly responsible for overseeing the development of Federal civilian agencies' cybersecurity programs, including monitoring and incident response. The memorandum also states that DHS activities will include:

1. overseeing the government-wide and agency-specific implementation of and reporting on cybersecurity policies and guidance;
2. overseeing and assisting government-wide and agency-specific efforts to provide adequate, risk-based and cost-effective cybersecurity;
3. overseeing the agencies' compliance with Federal Information Security Management Act (FISMA) and developing analyses for OMB to assist in the development of the FISMA annual report;
4. overseeing the agencies' cybersecurity operations and incident response and providing appropriate assistance; and
5. annually reviewing the agencies' cybersecurity programs.

On January 8, 2008, the Administration released the directive that established the United States policy, strategy, guidelines, and implementation actions to secure cyberspace. The Directive strengthened and augmented existing policies for protecting the security and privacy of information entrusted to the Federal Government and clarifies roles and responsibilities of Federal agencies relating to cybersecurity.

The Directive clarifies Federal roles and responsibilities in cyberspace and states. "the Secretary of Homeland Security shall lead the National effort to protect, defend, and reduce vulnerabilities of Federal systems." Specifically, "the Secretary of Homeland Security shall:

"(a) Manage and oversee, through US—CERT, the external access points, including access to the Internet, for all Federal systems;

"(b) Provide consolidated intrusion detection, incident analysis, and cyber response capabilities to protect Federal agencies' external access points, including access to the Internet, for all Federal systems;

"(c) In coordination with the Director of OMB, set minimum operational standards for Federal Government Network Operations Centers (NOCs) and Security Operations Centers (SOCs) that enable DHS, through US—CERT, to direct the operation and defense of external access points, including Internet access points, for all Federal systems, which the Secretary will certify and enforce;

“(d) Utilize the National Infrastructure Protection Plan process, in accordance with HSPD–7, to disseminate cyber threat, vulnerability, mitigation, and warning information to improve the security and protection of critical infrastructure networks owned or operated by Federal agencies; State, local, and tribal governments; private industry; academia; and international partners.”

Additionally, the Directive states, “the heads of all Federal agencies, to the extent permitted by law and necessary for the effective implementation of the cybersecurity mission, shall support and collaborate with the Secretary of Homeland Security. Further, all Federal agencies shall align their own network operations and defense capabilities to provide DHS with visibility and insight into the status of their Federal systems and shall respond to DHS direction in areas related to network security, allowing DHS to effectively protect the Federal Government network enterprise. Federal agencies shall continue to execute their responsibilities to protect and defend their networks.”

According to testimony by the Government Accountability Office (GAO) on May 7, 2014, “we [GAO] agree that DHS should play a role in the operational aspects of federal cybersecurity. We [GAO] suggested in February 2013 that Congress consider legislation that would clarify roles and responsibilities for implementing and overseeing federal information security programs and for protecting the nation’s critical assets.”

According to the Administration’s May 2011 Cybersecurity Legislative Proposal, it calls for Congress to provide DHS with clear statutory authority to carry out this operational mission, while reinforcing the fundamental responsibilities of individual agencies to secure their networks, and preserving the policy and budgetary coordination oversight of OMB.

In April 2014, before the Senate Appropriations Subcommittee on Homeland Security, Deputy Under Secretary for Cybersecurity Phyllis Schneck testified, “The Department recently responded to a serious vulnerability, known as ‘Heartbleed,’ in the widely-used OpenSSL encryption software that protects the electronic traffic on a large number of websites and devices . . . Even with the rapid and coordinated Federal Government response to Heartbleed, the lack of clear and updated laws reflecting the roles and responsibilities of civilian network security caused unnecessary delays in the incident response.” Deputy Under Secretary Schneck further added that in many cases five to six days were lost in responding to the “Heartbleed” incident as a result.

H.R. 3696 addresses the GAO, the Administration, and DHS’ recommendations and clarifies that DHS be the lead agency responsible for Federal cybersecurity efforts and protection of the .gov domain.

Since 2010 the Federal Network Resilience (FNR) division within the DHS Cybersecurity and Communications (CS&C) at DHS has overseen and administered operational network security compliance for all Federal civilian information systems. Additionally, Congress has appropriated funds for DHS to carry out this mission in both the 112th and 113th Congresses a total of 17 times. The Committee believes that legislation is strongly needed to strengthen the security of Federal civilian information systems by utilizing existing resources that Congress has already appropriated and by vest-

ing statutory authorities in DHS which is currently managing such operational activities on a daily basis.

DHS' Einstein program provides the United States Computer Emergency Readiness Team (US-CERT) with a situational awareness snapshot of the health of the Federal Governments' information systems. Based upon agreements with participating Federal agencies, US-CERT installs systems at an agency's Internet access points to collect network flow data. The agencies are provided tools to analyze their collected data. In addition, the data is shared with US-CERT Security Operations Center, housed at the NCCIC, which aggregates it from all EINSTEIN participants to identify network anomalies spanning the Federal Government. EINSTEIN has been available to Federal agencies since 2004 through three progressively more sophisticated versions (I, II and III). The Committee expects that the codification of these authorities will allow for the continuation of the Einstein program.

The Continuous Diagnostic and Monitoring (CDM) program is currently administered by the Department of Homeland Security and is expected to be fully operational by 2016. The CDM program seeks to defend Federal, State, and local government IT networks from cybersecurity threats by providing continuous monitoring sensors (tools), diagnosis, mitigation tools and continuous monitoring-as-a-service to strengthen the security posture of government networks. The Committee expects that the codification of these authorities will allow for the continuation of the Continuous Diagnostics and Monitoring program.

(i) Recommendations Regarding New Agreements

This subsection requires the Secretary, not later than 180 days after the date of the enactment of H.R. 3696, submit to Congress recommendations on how to expedite the implementation of information sharing agreements for cybersecurity purposes between DHS and private sector entities. These recommendations will address the development and utilization of a scalable form that retains all privacy and other protections and any additional authorities or resources that may be needed to increase the number of new agreements between DHS and private sector entities.

Cooperative Research and Development Agreements (CRADA) are a commonly used technology transfer and information sharing mechanism between DHS and its private sector partners. The Federal Government may provide personnel, services, facilities, equipment, intellectual property, or other resources without reimbursement. The private sector may provide funds, personnel, services, facilities, equipment, and intellectual property or other resources toward efforts that are consistent with the private sector partner. However, private industry has been frustrated with the CRADA process because they take many months to be negotiated and finalized.

Sec. 104. National Cybersecurity and Communications Integration Center.

This subsection establishes the National Cybersecurity and Communications Integration Center (NCCIC), within the Department of Homeland Security to be a Federal civilian information-sharing interface to provide shared situational awareness and enable real-time, integrated, and operational actions by and among Federal,

State, local government entities, ISACs, private sector entities, and critical infrastructure owners and operators.

The National Cybersecurity and Communications Integration Center, within the DHS Office of Cybersecurity and Communications, serves as a centralized location where operational elements involved in cybersecurity and communications reliance are coordinated and integrated. NCCIC partners include all Federal departments and agencies; state, local, Tribal, and territorial governments; the private sector; and several international entities. It also provides cyber threat and vulnerability analysis, early warning, and incident response assistance for public and private sector parties.

The Committee expects the NCCIC to operate as the primary civilian interface for real-time cyber threat information sharing, and operate at the intersection of the private sector, law enforcement, intelligence, and defense communities, applying unique and valuable analytic perspectives, ensuring real-time shared situational awareness, conducting risk assessments, mitigating vulnerabilities and threats to civilian government and private sector critical infrastructure, and orchestrating synchronized response efforts while protecting the constitutional and privacy and civil liberty rights of Americans in both the cybersecurity and communications domains. The Committee expects that the establishment of the NCCIC will fulfill many of the Secretary's roles and responsibilities laid out in PPD-21.

The NCCIC's mission includes: Disseminating cyber threat and vulnerability analysis information; leading the protection of Federal civilian agencies in cyberspace; working closely together with critical infrastructure owners and operators to reduce risk; collaborating with State and local governments through the Multi-State Information Sharing and Analysis Center (MS-ISAC); cooperating with international partners to share information and respond to incidents; coordinating national response to significant cyber incidents in accordance with the National Cyber Incident Response Plan (NCIRP); analyzing data to develop and share actionable mitigation recommendations; creating and maintaining shared situational awareness among its partners and constituents; and orchestrating national protection, prevention, mitigation, and recovery activities associated with . . . cyber incidents

The Committee is supportive of the progress made at the NCCIC over the last several years in building its capability and capacity to conduct higher-level analysis, facilitate more actionable and comprehensive information sharing with its partners, and provide a more comprehensive approach to response, mitigation, and recovery efforts from cyber incidents. While progress has been made, the Committee believes that much work is still needed at the NCCIC to develop the essential capabilities to most effectively protect our Nation's critical infrastructure from a cyber attack. The Committee expects the NCCIC to continue its progress in collaborating with other Federal agencies and private sector partners to finding cost effective and innovative solutions to building a highly reputable state-of-the-art Federal civilian cybersecurity operations center. The Committee believes that in order to maximize the utility of cyber threat information sharing with the private sector, the Secretary must more effectively leverage private sector subject matter

expertise. These subject matter experts should provide advice regarding the content, function, and type of information most useful to critical infrastructure owners and operators in reducing and mitigating cyber risks.

(b) Composition

This subsection establishes the entities at the NCCIC to include at least one ISAC from each critical infrastructure sector, the MS-ISAC, the United States Computer Emergency Readiness Team (US-CERT), the Industrial Control System Cyber Emergency Response Team (ICS-CERT), the National Coordinating Center for Telecommunications, and such Federal, State, local private entities, organizations, or individuals the Secretary considers appropriate that agree to be included.

The 16 critical infrastructure ISACs will serve as an information sharing resource for each sector and promote on-going multi-directional sharing of real-time, relevant and actionable cyber threat information and analysis by and among each sector, the Department, Sector-Specific Agencies, and other critical infrastructure ISACs. The ISACs serve as the primary private sector interface with the NCCIC. Today, there are a limited amount of critical infrastructure sectors that are permanent residents on the floor of the NCCIC. The Committee believes there is significant value in having all critical infrastructure sectors represented on the NCCIC floor. This will not only increase real-time information sharing and threat analysis, but also help foster stronger partnerships across all 16 critical infrastructure sectors. As such, the Committee expects that all 16 recognized ISACs will be physically located on the NCCIC floor.

The MS-ISAC collaborates with State and local governments to protect from, prevent, mitigate, respond to, and recover from cyber incidents.

US-CERT leads efforts to improve the Nation's cybersecurity posture, coordinate information sharing, and proactively manage cyber risks to the Nation while protecting the constitutional rights of Americans. Through its 24 hours a day, 7 days a week operations center, US-CERT distributes vulnerability and threat information and operates a database to provide technical descriptions of system vulnerabilities. US-CERT also partners with private sector critical infrastructure owners and operators, academia, federal agencies, ISACs, state and local partners, and domestic and international organizations to enhance the Nation's cybersecurity posture.

ICS-CERT coordinates with industrial control systems owners and operators and shares industrial control systems-related security incidents and mitigation measures to protect from, prevent, mitigate, respond to, and recover from cyber incidents.

The National Coordinating Center for Telecommunications coordinates the protection, response, and recovery of national security emergency communications.

(c) Cyber Incident

This subsection enables the Secretary to grant Federal, State, local governments, private entities, and critical infrastructure owners and operators immediate temporary access to the NCCIC in the event of a cyber incident.

While a particular entity may not have daily access to the NCCIC floor, the Committee believes it is critical for certain entities to be granted temporary access to the NCCIC in the event of a cyber incident, so that any affected entity can be in the best position to be privy to real-time cyber threat information and have situational awareness related to the incident.

(d) Roles and Responsibilities

This subsection enables the NCCIC to promote ongoing multi-directional sharing of actionable cyber threat information and analysis on a real time basis; facilitate cross sector coordination and sharing of cyber threat information; provide, upon request, timely technical assistance and crisis management support; coordinate with other Federal agencies to reduce redundant reporting of cyber threat information; collaborate with Sector Coordinating Councils, Information Sharing and Analysis Centers, Sector Specific Agencies, and the relevant critical infrastructure sectors on procedures to support real-time information sharing capabilities and mechanisms; cooperate with international partners to share information and respond to cyber incidents within the scope of relevant treaties; safeguard sensitive cyber threat information from unauthorized disclosure; and perform other duties as assigned by the Secretary. The Secretary shall implement policies and procedures to provide technical assistance to Federal civilian agencies to prevent and respond to data breaches involving personally identifiable information (PII) that occur on Federal civilian systems. This section requires reporting by Federal civilian agencies to notify the NCCIC about unauthorized acquisition or access of PII that occur on Federal civilian systems not later than two business days after the discovery of a breach. The Secretary shall require those agencies to notify all potential victims of a data breach involving PII without reasonable delay consistent with the needs of law enforcement.

The NCCIC is the Federal civilian interface to the owners and operators of the Nation's critical infrastructure for cyber threat information sharing. This civilian interface affords industry and private sector entities the opportunity to share cyber threat information with the Federal Government without the concerns they may have in sharing such information with the U.S. intelligence community or the Department of Defense. DHS, as a civilian agency, complies with substantive privacy and civil liberties protections, which create a safe harbor for stakeholders. In fact, the first statutorily created Chief Privacy Officer position was established at DHS. As the need for the sharing of cyber threat information between the Federal Government and industry became apparent, the NCCIC naturally evolved out of the robust public-private partnership between DHS and critical infrastructure established by the principles of the National Infrastructure Protection Plan.

While DHS should be the primary interface between the Federal Government and the private sector, H.R. 3696 does not preclude appropriate relationships between the private sector and other Federal entities.

H.R. 3696 encourages the private sector to share information with the Federal Government, however, there is no mandatory information-sharing requirement placed on the private sector under this legislation.

The Committee sees the NCCIC functioning and serving as an information sharing interface with the private sector in a “hub and spoke” model where the NCCIC is composed of 16 critical infrastructure sector ISAC partners.

(e) Integration and Analysis

This subsection enables the NCCIC, in coordination with the Office of Integration and Analysis, to integrate and analyze cyber threat information it receives; assess and evaluate consequence, vulnerability, and threat information to share with entities actionable risks from cyber incidents; and to assist critical infrastructure owners and operators by making recommendations to facilitate improvements to the security and resiliency of the critical infrastructure of the United States.

The Committee agrees with PPD–21’s statement that the implementation of an integration and analysis function to inform planning and operations decisions regarding critical infrastructure is imperative to strengthening critical infrastructure security and resilience.

The Committee believes that the NCCIC needs to increase its production of high-value cross sector analysis of cyber threat information and disseminate that analysis to its public and private partners in near-real time. It is the Committee’s expectation that with increased information sharing and personnel resources at the NCCIC, the NCCIC will be able to produce a greater number of high-value analysis products.

(f) Report of Cyber Attacks Against Federal Government Networks

This subsection requires the Secretary of Homeland Security to submit an annual report to Congress summarizing major cyber incidents involving Federal civilian information systems and provide aggregate statistics on the number of breaches, the volume of data exfiltrated, the consequential impact, extent of any personally identifiable information (PII) that was involved, and the estimated cost of remedying such breaches.

The Committee would like greater situational awareness of cyber incidents on Federal civilian information systems and more information on how the NCCIC is responding to these data breaches.

(g) Report on the Operations of the Center

This subsection requires the Secretary, in consultation with the Sector Coordinating Councils and appropriate Federal Government agencies, to submit an annual report to Congress on the capability and capacity of the NCCIC to carry out its cybersecurity mission and the extent to which the Department is engaged in the sharing of cyber threat information with each critical infrastructure sector. This section also requires that no later than one year after enactment, the Government Accountability Office will report to Congress on the effectiveness of the NCCIC to carry out its cybersecurity mission.

The NCCIC, as the Federal civilian interface with critical infrastructure plays a critical role in cyber information sharing. The Committee feels strongly that annual verification of its capability and capacity to carry out its mission is imperative to build NCCIC’s credibility and ensure that taxpayer dollars are being used wisely.

Sec. 105. Cyber incident response and technical assistance.

This section requires the Secretary to establish Cyber Incident Response Teams to provide, upon request, timely technical assistance, and crisis management support, and actionable recommendations on security and resilience measures prior to, during and after cyber incidents to critical infrastructure owners and operators. This section also requires the Secretary to develop a National Cybersecurity Incident Response Plan to coordinate among stakeholders ensuring it is regularly updated, maintained and exercised.

Additionally, the Secretary shall regularly update, maintain, and exercise the Cyber Incident Response Annex to the National Response Framework. While the Committee does not intend to dictate how often the Annex is updated, the Committee does expect that the Annex will be updated as necessary and at least more than once every ten years, which is nearly the time elapsed since the previous update. The Committee expects that DHS will be prepared for any scenario of a cyber attack on U.S. critical infrastructure, and has operationalized how DHS will effectively coordinate with other Federal, State, local, Tribal, and private sector stakeholders in mitigating, responding, and recovering from a cyber attack on U.S. critical infrastructure.

DHS has capable resources to assist critical infrastructure stakeholders in the event of a cyber incident small or large. The cyber incident response teams are proving to be extraordinarily helpful to those stakeholders who have voluntarily sought their assistance. There is absolutely nothing in this provision that requires any private entity to either seek or accept assistance from DHS cyber incident response teams.

Sec. 106. Streamlining of Department cybersecurity organization.

This section renames the Department's "National Protection and Programs Directorate" as the "Cybersecurity and Infrastructure Protection Directorate," and codifies an Under Secretary for Cybersecurity and Infrastructure Protection, a Deputy Under Secretary for Cybersecurity, and a Deputy Under Secretary for Infrastructure Protection. This section also requires the Secretary to submit a report to Congress on the feasibility of making the Department's Cybersecurity and Communications Office an operational component of the Department and recommendations for restructuring the SAFETY Act office to protect and maintain operations in accordance with the office's mission to provide incentives for the development and deployment of anti-terrorism technologies while elevating the profile and mission of the office. This section also requires the Secretary to assess the effectiveness of acquisition processes and the use of existing authorities for acquiring cybersecurity technologies. Finally, the Secretary shall make Department contact information available to Sector Coordinating Councils, critical infrastructure owners, and critical infrastructure operators to coordinate cybersecurity emergency response and recovery efforts.

The Committee believes that a core function of the SAFETY Act Office, the evaluation of anti-terrorism technologies, should not be diminished or curtailed as a result of this legislation and, for that reason, requires the Department to provide recommendations for restructuring the Office.

TITLE II—PUBLIC-PRIVATE COLLABORATION ON CYBERSECURITY

Sec. 201. Public-private collaboration on cybersecurity.

This section requires that National Institute of Standards and Technology (NIST), in coordination with the Secretary, on an ongoing basis, to facilitate and support the development of a voluntary, industry-led set of standards, guidelines, best practices, methodologies, and procedures to reduce cyber risks to critical infrastructure. The Department and NIST are expected to work closely with critical infrastructure owners, critical infrastructure operators, Sector Coordinating Councils, Information Sharing Analysis Centers, Sector Specific Agencies, relevant industry organizations and other Federal, State, local, and international governments to accomplish these goals. This section prohibits the prescription or requirement of specific solutions or specific technology products. In addition, any information shared with DHS of NIST may not be used for regulatory purposes.

(a) Meetings

This subsection requires the Secretary to meet with the Sector Coordinating Council for each critical infrastructure sector on a bi-annual basis to engage in dialogue about ideas to improve cybersecurity for the critical infrastructure sectors. The Secretary shall inform each Sector Coordinating Council of threat assessments to each sector and provide voluntary recommendations to improve critical infrastructure at each meeting.

The Committee strongly believes that increasing cybersecurity for critical infrastructure can only be achieved through a continuous dialogue between the private sector and the Federal Government. Meetings between the Sector Coordinating Councils and the Secretary, required under this section, are designed to foster a more seamless collaboration between DHS and critical infrastructure.

(b) Report

Based on discussions at the meetings between the Department and the Sector Coordinating Councils, the Secretary is required by this subsection to submit to Congress an annual report on the state of cybersecurity for each critical infrastructure sector. This section also requires the Secretary to provide a draft of each report to the Sector Coordinating Council for each critical infrastructure sector before submitting the report to Congress. In the event such Sector Coordinating Council provides a written response, this section requires the Secretary to include such written response in the final report to Congress. Furthermore, the Secretary is required to maintain a public copy of each report and each report shall include a non-public annex for proprietary, business-sensitive information or other sensitive information. Each report is expected to include the known risks to each critical infrastructure sector, any cyber incidents that occurred during the previous year, and the volume of voluntary technical assistance sought.

(c) Limitation

This subsection states that information shared with or provided to Sector Coordinating Council, a critical infrastructure sector, or the Secretary for the purpose of the activities under subsections (a)

and (b) shall not be used by any Federal, State, or local government department or agency to regulate the activity of any private entity.

Sec. 202. SAFETY Act and qualifying cyber incidents.

The “Support Anti-terrorism by Fostering Effective Technologies Act of 2002,” or SAFETY Act (subtitle G of the Homeland Security Act of 2002, Pub. L. 107–296), limits liability for a “qualified anti-terrorism technology” used in an “act of terrorism.” Section 202 of H.R. 3696 clarifies that “act of terrorism” as defined in the SAFETY Act includes “cybersecurity technology” used in a “qualifying cyber incident.”

The intent of clarifying the liability protections of the SAFETY Act is to provide an incentive for companies to be innovative in developing methods and technologies for defending against, responding to, recovering from, mitigating, or otherwise combating cyber attacks, as well as to help ensure the widespread deployment of such items. It is important that the SAFETY Act undertake comprehensive assessment of cybersecurity technologies seeking legal protections as it does for other anti-terrorism technologies.

Further, the Committee encourages the Secretary, when making a declaration of a “qualifying cyber incident,” to communicate to Congress and the American people the rationale behind and basis of any such declaration, to the extent that it does not jeopardize homeland security or national security.

The Committee understands that the Science and Technology Directorate has been using contractors for at least the last 10 years to assist the Office of SAFETY Act Implementation (OSAI) with the review of SAFETY Act applications. It is also the Committee’s understanding that the budget for such outside contractors constitutes a significant portion of OSAI’s annual budget. Given continued financial pressures on the Science and Technology Directorate, on-going questions regarding the performance of the contractors, and the potential increase in SAFETY Act applications submitted to OSAI, the Science and Technology Directorate shall include the feasibility of using outside contractors to evaluate SAFETY Act applications.

Sec. 203. Prohibition on new regulatory authority.

This section requires that nothing in this Act or its amendments (except that this section shall not apply in the case of section 202 of this Act and the amendments made by such section 202) can create any new regulations, provide additional regulatory authority, or permit regulatory actions that would duplicate, conflict with or supersede existing regulatory requirements.

The Committee understands that many critical infrastructure owners and operators have taken steps, and will continue to shore up their cybersecurity defenses and create internal cybersecurity procedures. The Committee believes that the Federal Government can best bolster these cybersecurity efforts, by fostering greater information sharing between the Federal Government and critical infrastructure through the NCCIC and greater collaboration between private and public entities.

Sec. 204. Prohibition on additional authorization of appropriations.

This section requires that no additional funds are authorized to be appropriated to carry out H.R. 3696 and amendments made by H.R. 3696, and such amendments shall be carried out using amounts that have already been appropriated.

Sec. 205. Prohibition on collection activities to track individuals' personally identifiable information.

This section requires that nothing in H.R. 3696 shall permit the Department to engage in the monitoring, surveillance, exfiltration or other collection activities to track and individual's personally identifiable information (PII).

The Committee expects that the Department will carry out this provision by following the agreed upon Fair Information Practice Principles (FIPP).

Over the past quarter century, government agencies in the United States, Canada, and Europe have studied the manner in which entities collect and use personal information—their “information practices”—and the safeguards required to assure those practices are fair and provide adequate privacy protection. The result has been a series of reports, guidelines, and model codes that represent widely accepted principles concerning fair information practices.

Additionally, the FIPPs are rooted in the tenets of the Privacy Act of 1974 and provide a framework through which to assess the nature of and the purpose for which data is collected. The Committee believes that the FIPPs are an essential component of civilian cybersecurity privacy protection efforts and expects that the Department will continue to follow and use the FIPPs as the foundational principles for privacy policy implementations pertaining to cybersecurity. These principles are: Transparency, individual participation, purpose specification, data minimization, use limitation, data quality and integrity, security, and accountability and auditing.

The Department of Homeland Security Privacy Office is the first statutorily required privacy office in any Federal agency, responsible for evaluating Department programs, systems, and initiatives for potential privacy impacts, and providing mitigation strategies to reduce the privacy impact. The Privacy Office works with every component and program to ensure that privacy considerations are addressed when planning or updating any program, system or initiative and uses the DHS FIPPs as the policy framework to enhance privacy protections by assessing the nature and purpose for all personally identifiable information (PII) collected to fulfill the Department's mission. Additionally, the Privacy Office: Evaluates Department legislative and regulatory proposals involving collection, use, and disclosure of PII; centralizes FOIA and Privacy Act operations to provide policy and programmatic oversight, and support implementation across the Department; operates a Department-wide Privacy Incident Response Program to ensure that incidents involving PII are properly reported, investigated and mitigated, as appropriate; responds to complaints of privacy violations and provides redress, as appropriate; and provides training, education and outreach to build a culture of privacy across the Department and transparency to the public.

The DHS Privacy Office is often involved in reviewing potential cybersecurity programs from their very inception rather than being

brought in later to “rubber stamp” or “fix” programs. Also, the Secretary and the Chief Privacy Officer have created the DHS Data Privacy and Integrity Advisory Committee. This group of outside, industry leaders brings additional transparency to the privacy process.

In accordance with Executive Order 13636, Section 5, the Committee expects that DHS’s Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties will be leveraged to ensure privacy and civil liberties are adequately protected for all cybersecurity information sharing policies and procedures.

The fact that the American Civil Liberties Union characterized the Committee-approved bill as “pro-security and pro-privacy” underscores the legislation’s preservation of existing privacy laws for cybersecurity.

The Office of Cybersecurity and Communications (CS&C) established a formal Oversight and Compliance Officer, to oversee all information handling requirements, policies, and procedures, including those, which protect privacy, and civil rights and civil liberties. This official fulfills this responsibility by auditing and inspecting information practices to ensure functions are executed in conformance with legal and policy objectives. The CS&C official is also available to consult with DHS components as a subject matter expert in planning and executing cybersecurity activities that touch upon privacy and information handling. Moreover, the official is also the a liaison to the Department’s Chief Privacy Office and the DHS Office for Civil Rights and Civil Liberties, thus ensuring that privacy, civil rights, and civil liberty concerns are interwoven into all aspects of cybersecurity planning and execution. The Committee expects that these activities will be incorporated into all cybersecurity activities at the Department.

Sec. 206. Cybersecurity scholars.

This section directs the Secretary to determine the feasibility and benefit of the development of a visiting security researchers program from educational institutions and cybersecurity scholars at the Department’s Centers of Excellence.

Sec. 207. National Research Council study on the resilience and reliability of the Nation’s power grid.

This section requires the National Research Council to research and report options for improving the Nation’s ability to expand and strengthen the capabilities of the power grid, including estimates of cost, time scale for implementation, and identification of any potential significant health and environmental impacts. The research would consider technical, economic, regulatory, environmental, and geopolitical factors likely to affect the efficiency and reliability of operations, as well as the ability of the grid to recover from disruptions (including acts of terrorism and cyber incidents). The Secretary shall make available to the National Research Council all appropriate information and personnel while conducting this research. The Committee expects any previous research done in this area shall be leveraged to expedite the release of the report and preserve resources.

TITLE III—HOMELAND SECURITY CYBERSECURITY WORKFORCE

Sec. 301. Homeland security cybersecurity workforce.

(a) Short Title

This title may be referred to as the “Homeland Security Cybersecurity Boots-on-the-Ground Act.”

(b) Cybersecurity Occupation Categories

This subsection requires the Secretary to develop and issue comprehensive occupation classifications for persons performing activities in furtherance of the Department’s cybersecurity missions. The Secretary shall ensure that the classifications are used throughout the Department and made available to other Federal agencies. These comprehensive classifications must be made no later than 90 days after the enactment of this Act.

This provision is informed by the work of the Homeland Security Advisory Committee (HSAC) “Task Force on CyberSkills” which issued a series of recommendations that include the adoption and maintenance of an authoritative list of mission-critical cybersecurity tasks and the adoption of a sustainable model for assessing the competency and progress of the existing and future DHS mission-critical cybersecurity workforce.

(c) Cybersecurity Workforce Assessment

This subsection requires the Secretary, to assess the readiness and capacity of the Department to meet its cybersecurity mission. The Committee expects such assessment to be conducted in collaboration with the Chief Human Capital Officer and Chief Information Officer of the Department. This assessment must be conducted no later than 180 days after the enactment of this Act. The assessment shall, at a minimum, include the following: Information where cybersecurity positions are located within the Department; information on which cybersecurity positions are performed by permanent full time departmental employees, individuals employed by independent contractors, and individuals employed by other Federal agencies; the number of individuals hired by the Department pursuant to the authority granted to the Secretary in 2009 to permit the Secretary to fill 1,000 cybersecurity positions over a three year period; information on vacancies within the Department’s cybersecurity supervisory workforce; information on the percentage of individuals within each cybersecurity occupation classification who received essential training to perform their jobs; and information on recruiting costs incurred with respect to efforts to fill cybersecurity positions across the Department.

(d) Workforce Strategy

In this subsection, the contents of the workforce strategy are prescribed. This subsection requires the Secretary, not later than 180 days after the enactment of this Act, to develop a comprehensive workforce strategy that enhances the readiness, capacity, training, and recruitment and retention of the Department’s cybersecurity workforce. This workforce strategy shall include a multiphase recruitment plan, a 5-year implementation plan, and a 10-year projection of Federal workforce needs. By including a specific timeframe, the Committee encourages DHS to address near-term, mid-

term, and long-term aspects of the plan. The workforce strategy is to be developed in a manner that is not constrained by fiscal resources to address both short-term and long-term strategies. The Committee expects that this workforce strategy will provide a comprehensive roadmap on how DHS plans to leverage its workforce resources to build up the capability and capacity at the NCCIC to be a highly reputable and state-of-the-art cybersecurity operations center.

(e) Information Security Training

This subsection sets forth the requirements for information security training of the cybersecurity workforce. It requires the Secretary to establish and maintain a process to verify that individuals employed by independent contractors who serve in cybersecurity positions at the Department receive initial and recurrent information security training. The Secretary shall maintain documentation to ensure that training provided to an individual meets or exceeds requirements for such individual's job function.

The Department, like other Federal agencies, utilizes outside contractors in its cybersecurity operations. In light of high-profile incidents where individuals employed by such firms improperly handled classified or otherwise sensitive information, the Committee believes that ensuring information security training is provided to individuals working on Department systems is essential.

(f) Updates

This subsection requires the Secretary to provide updates regarding the cybersecurity workforce assessment, information on the progress of carrying out the comprehensive workforce strategy, and information on the status of the implementation of information security training.

(g) GAO Study

This subsection requires the Secretary to provide the Comptroller General of the United States information on the cybersecurity workforce assessment and progress on carrying out the comprehensive workforce strategy developed. This subsection also requires the GAO to submit to the relevant congressional committees a study on such assessment and strategies. The Committee's intent of this subsection is to direct GAO to gather data and evaluate DHS's workforce assessment and strategies.

(h) Cybersecurity Fellowship Program

This subsection requires the Secretary to submit to the appropriate committees of Congress a report on the feasibility of establishing a Cybersecurity Fellowship Program to offer a tuition payment plan for undergraduate and doctoral candidates who agree to work for the Department for an agreed-upon period of time.

Sec. 302. Personnel authorities.

This section enables the Department to use the same authority as the Department of Defense with respect to establishing cybersecurity positions in the "excepted service" if the Secretary determines that such is needed to retain essential cybersecurity personnel. This section also requires the Secretary to submit to Congress a report within 120 days that contains a plan for the use of these authorities. This section also requires an annual report for four consecutive years that discusses the process used by the Sec-

retary in implementing this section and accepting applications and assessing candidates for employment.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, existing law in which no change is proposed is shown in roman):

HOMELAND SECURITY ACT OF 2002

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) * * *

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

* * * * *

TITLE II—INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION

* * * * *

【Subtitle C—Information Security】

Subtitle C—Cybersecurity and Information Sharing

* * * * *

Sec. 226. Enhancement of cybersecurity.

Sec. 227. Protection of critical infrastructure and information sharing.

Sec. 228. National Cybersecurity and Communications Integration Center.

Sec. 229. Cyber incident response and technical assistance.

Sec. 230. Public-private collaboration on cybersecurity.

Sec. 230A. Cybersecurity occupation categories, workforce assessment, and strategy.

Sec. 230B. Personnel authorities.

* * * * *

SEC. 2. DEFINITIONS.

In this Act, the following definitions apply:

(1) * * *

* * * * *

(19) The term “critical infrastructure” has the meaning given that term in section 1016(e) of the USA Patriot Act (42 U.S.C. 5195c(e)).

(20) The term “critical infrastructure owner” means a person that owns critical infrastructure.

(21) The term “critical infrastructure operator” means a critical infrastructure owner or other person that manages, runs, or operates, in whole or in part, the day-to-day operations of critical infrastructure.

(22) The term “cyber incident” means an incident, or an attempt to cause an incident, that, if successful, would—

(A) jeopardize or imminently jeopardize, without lawful authority, the security, integrity, confidentiality, or availability of an information system or network of information systems or any information stored on, processed on, or transiting such a system or network;

(B) constitute a violation or imminent threat of violation of law, security policies, security procedures, or acceptable

use policies related to such a system or network, or an act of terrorism against such a system or network; or

(C) result in the denial of access to or degradation, disruption, or destruction of such a system or network, or the defeat of an operations control or technical control essential to the security or operation of such a system or network.

(23) The term “cybersecurity mission” means activities that encompass the full range of threat reduction, vulnerability reduction, deterrence, incident response, resiliency, and recovery activities to foster the security and stability of cyberspace.

(24) The term “cybersecurity purpose” means the purpose of ensuring the security, integrity, confidentiality, or availability of, or safeguarding, an information system or network of information systems, including protecting such a system or network, or data residing on such a system or network, including protection of such a system or network, from—

(A) a vulnerability of such a system or network;

(B) a threat to the security, integrity, confidentiality, or availability of such a system or network, or any information stored on, processed on, or transiting such a system or network;

(C) efforts to deny access to or degrade, disrupt, or destroy such a system or network; or

(D) efforts to gain unauthorized access to such a system or network, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting such a system or network.

(25) The term “cyber threat” means any action that may result in unauthorized access to, exfiltration of, manipulation of, harm of, or impairment to the security, integrity, confidentiality, or availability of an information system or network of information systems, or information that is stored on, processed by, or transiting such a system or network.

(26) The term “cyber threat information” means information directly pertaining to—

(A) a vulnerability of an information system or network of information systems of a government or private entity;

(B) a threat to the security, integrity, confidentiality, or availability of such a system or network of a government or private entity, or any information stored on, processed on, or transiting such a system or network;

(C) efforts to deny access to or degrade, disrupt, or destroy such a system or network of a government or private entity;

(D) efforts to gain unauthorized access to such a system or network, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting such a system or network; or

(E) an act of terrorism against an information system or network of information systems.

(27) The term “Federal civilian information systems”—

(A) means information, information systems, and networks of information systems that are owned, operated, controlled, or licensed for use by, or on behalf of, any Fed-

eral agency, including such systems or networks used or operated by another entity on behalf of a Federal agency; but (B) does not include—

(i) a national security system; or

(ii) information, information systems, and networks of information systems that are owned, operated, controlled, or licensed solely for use by, or on behalf of, the Department of Defense, a military department, or an element of the intelligence community.

(28) The term “information security” means the protection of information, information systems, and networks of information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

(A) integrity, including guarding against improper information modification or destruction, including ensuring nonrepudiation and authenticity;

(B) confidentiality, including preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

(C) availability, including ensuring timely and reliable access to and use of information.

(29) The term “information system” means the underlying framework and functions used to process, transmit, receive, or store information electronically, including programmable electronic devices, communications networks, and industrial or supervisory control systems and any associated hardware, software, or data.

(30) The term “private entity” means any individual or any private or publically-traded company, public or private utility (including a utility that is a unit of a State or local government, or a political subdivision of a State government), organization, or corporation, including an officer, employee, or agent thereof.

(31) The term “shared situational awareness” means an environment in which cyber threat information is shared in real time between all designated Federal cyber operations centers to provide actionable information about all known cyber threats.

* * * * *

TITLE I—DEPARTMENT OF HOMELAND SECURITY

* * * * *

SEC. 103. OTHER OFFICERS.

(a) DEPUTY SECRETARY; UNDER SECRETARIES.—(1) IN GENERAL.—Except as provided under paragraph (2), there are the following officers, appointed by the President, by and with the advice and consent of the Senate:

(A) * * *

* * * * *

(K) Under Secretary for Cybersecurity and Infrastructure Protection.

(L) Deputy Under Secretary for Cybersecurity.

(M) Deputy Under Secretary for Infrastructure Protection.

* * * * *

TITLE II—INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION

* * * * *

Subtitle C—[Information Security] *Cybersecurity and Information Sharing*

* * * * *

SEC. 226. ENHANCEMENT OF CYBERSECURITY.

The Secretary, in collaboration with the heads of other appropriate Federal Government entities, shall conduct activities for cybersecurity purposes, including the provision of shared situational awareness to each other to enable real-time, integrated, and operational actions to protect from, prevent, mitigate, respond to, and recover from cyber incidents.

SEC. 227. PROTECTION OF CRITICAL INFRASTRUCTURE AND INFORMATION SHARING.

(a) PROTECTION OF CRITICAL INFRASTRUCTURE.—

(1) IN GENERAL.—The Secretary shall coordinate, on an ongoing basis, with Federal, State, and local governments, national laboratories, critical infrastructure owners, critical infrastructure operators, and other cross sector coordinating entities to—

(A) facilitate a national effort to strengthen and maintain secure, functioning, and resilient critical infrastructure from cyber threats;

(B) ensure that Department policies and procedures enable critical infrastructure owners and critical infrastructure operators to receive real-time, actionable, and relevant cyber threat information;

(C) seek industry sector-specific expertise to—

(i) assist in the development of voluntary security and resiliency strategies; and

(ii) ensure that the allocation of Federal resources are cost effective and reduce any burden on critical infrastructure owners and critical infrastructure operators;

(D) upon request of entities, facilitate and assist risk management efforts of such entities to reduce vulnerabilities, identify and disrupt threats, and minimize consequences to their critical infrastructure;

(E) upon request of critical infrastructure owners or critical infrastructure operators, provide education and assistance to such owners and operators on how they may use protective measures and countermeasures to strengthen the security and resilience of the Nation's critical infrastructure; and

(F) coordinate a research and development strategy to facilitate and promote advancements and innovation in cybersecurity technologies to protect critical infrastructure.

(2) *ADDITIONAL RESPONSIBILITIES.—The Secretary shall—*

(A) manage Federal efforts to secure, protect, and ensure the resiliency of Federal civilian information systems using a risk-based and performance-based approach, and, upon request of critical infrastructure owners or critical infrastructure operators, support such owners' and operators' efforts to secure, protect, and ensure the resiliency of critical infrastructure from cyber threats;

(B) direct an entity within the Department to serve as a Federal civilian entity by and among Federal, State, and local governments, private entities, and critical infrastructure sectors to provide multi-directional sharing of real-time, actionable, and relevant cyber threat information;

(C) build upon existing mechanisms to promote a national awareness effort to educate the general public on the importance of securing information systems;

(D) upon request of Federal, State, and local government entities and private entities, facilitate expeditious cyber incident response and recovery assistance, and provide analysis and warnings related to threats to and vulnerabilities of critical information systems, crisis and consequence management support, and other remote or on-site technical assistance with the heads of other appropriate Federal agencies to Federal, State, and local government entities and private entities for cyber incidents affecting critical infrastructure;

(E) engage with international partners to strengthen the security and resilience of domestic critical infrastructure and critical infrastructure located outside of the United States upon which the United States depends; and

(F) conduct outreach to educational institutions, including historically black colleges and universities, Hispanic serving institutions, Native American colleges, and institutions serving persons with disabilities, to encourage such institutions to promote cybersecurity awareness.

(3) *RULE OF CONSTRUCTION.—Nothing in this section may be construed to require any private entity to request assistance from the Secretary, or require any private entity requesting such assistance to implement any measure or recommendation suggested by the Secretary.*

(b) *CRITICAL INFRASTRUCTURE SECTORS.—The Secretary, in collaboration with the heads of other appropriate Federal agencies, shall designate critical infrastructure sectors (that may include subdivisions of sectors within a sector as the Secretary may determine appropriate). The critical infrastructure sectors designated under this subsection may include the following:*

- (1) *Chemical.*
- (2) *Commercial facilities.*
- (3) *Communications.*
- (4) *Critical manufacturing.*
- (5) *Dams.*
- (6) *Defense Industrial Base.*

- (7) *Emergency services.*
- (8) *Energy.*
- (9) *Financial services.*
- (10) *Food and agriculture.*
- (11) *Government facilities.*
- (12) *Healthcare and public health.*
- (13) *Information technology.*
- (14) *Nuclear reactors, materials, and waste.*
- (15) *Transportation systems.*
- (16) *Water and wastewater systems.*
- (17) *Such other sectors as the Secretary determines appropriate.*

(c) *SECTOR SPECIFIC AGENCIES.*—The Secretary, in collaboration with the relevant critical infrastructure sector and the heads of other appropriate Federal agencies, shall recognize the Federal agency designated as of November 1, 2013, as the “Sector Specific Agency” for each critical infrastructure sector designated under subsection (b). If the designated Sector Specific Agency for a particular critical infrastructure sector is the Department, for the purposes of this section, the Secretary shall carry out this section. The Secretary, in coordination with the heads of each such Sector Specific Agency shall—

- (1) *support the security and resilience activities of the relevant critical infrastructure sector in accordance with this subtitle; and*
- (2) *provide institutional knowledge and specialized expertise to the relevant critical infrastructure sector.*

(d) *SECTOR COORDINATING COUNCILS.*—

(1) *RECOGNITION.*—The Secretary, in collaboration with each critical infrastructure sector and the relevant Sector Specific Agency, shall recognize and partner with the Sector Coordinating Council for each critical infrastructure sector designated under subsection (b) to coordinate with each such sector on security and resilience activities and emergency response and recovery efforts.

(2) *MEMBERSHIP.*—

(A) *IN GENERAL.*—The Sector Coordinating Council for a critical infrastructure sector designated under subsection (b) shall—

- (i) *be comprised exclusively of relevant critical infrastructure owners, critical infrastructure operators, private entities, and representative trade associations for the sector;*
- (ii) *reflect the unique composition of each sector; and*
- (iii) *include relevant small, medium, and large critical infrastructure owners, critical infrastructure operators, private entities, and representative trade associations for the sector.*

(B) *PROHIBITION.*—No government entity with regulating authority shall be a member of the Sector Coordinating Council.

(C) *LIMITATION.*—The Secretary shall have no role in the determination of the membership of a Sector Coordinating Council.

(3) *ROLES AND RESPONSIBILITIES.*—*The Sector Coordinating Council for a critical infrastructure sector shall—*

(A) *serve as a self-governing, self-organized primary policy, planning, and strategic communications entity for coordinating with the Department, the relevant Sector-Specific Agency designated under subsection (c), and the relevant Information Sharing and Analysis Centers under subsection (e) on security and resilience activities and emergency response and recovery efforts;*

(B) *establish governance and operating procedures, and designate a chairperson for the sector to carry out the activities described in this subsection;*

(C) *coordinate with the Department, the relevant Information Sharing and Analysis Centers under subsection (e), and other Sector Coordinating Councils to update, maintain, and exercise the National Cybersecurity Incident Response Plan in accordance with section 229(b); and*

(D) *provide any recommendations to the Department on infrastructure protection technology gaps to help inform research and development efforts at the Department.*

(e) *SECTOR INFORMATION SHARING AND ANALYSIS CENTERS.*—

(1) *RECOGNITION.*—*The Secretary, in collaboration with the relevant Sector Coordinating Council and the critical infrastructure sector represented by such Council, and in coordination with the relevant Sector Specific Agency, shall recognize at least one Information Sharing and Analysis Center for each critical infrastructure sector designated under subsection (b) for purposes of paragraph (3). No other Information Sharing and Analysis Organizations, including Information Sharing and Analysis Centers, may be precluded from having an information sharing relationship within the National Cybersecurity and Communications Integration Center established pursuant to section 228. Nothing in this subsection or any other provision of this subtitle may be construed to limit, restrict, or condition any private entity or activity utilized by, among, or between private entities.*

(2) *ROLES AND RESPONSIBILITIES.*—*In addition to such other activities as may be authorized by law, at least one Information Sharing and Analysis Center for a critical infrastructure sector shall—*

(A) *serve as an information sharing resource for such sector and promote ongoing multi-directional sharing of real-time, relevant, and actionable cyber threat information and analysis by and among such sector, the Department, the relevant Sector Specific Agency, and other critical infrastructure sector Information Sharing and Analysis Centers;*

(B) *establish governance and operating procedures to carry out the activities conducted under this subsection;*

(C) *serve as an emergency response and recovery operations coordination point for such sector, and upon request, facilitate cyber incident response capabilities in coordination with the Department, the relevant Sector Specific Agency and the relevant Sector Coordinating Council;*

(D) facilitate cross-sector coordination and sharing of cyber threat information to prevent related or consequential impacts to other critical infrastructure sectors;

(E) coordinate with the Department, the relevant Sector Coordinating Council, the relevant Sector Specific Agency, and other critical infrastructure sector Information Sharing and Analysis Centers on the development, integration, and implementation of procedures to support technology neutral, real-time information sharing capabilities and mechanisms within the National Cybersecurity and Communications Integration Center established pursuant to section 228, including—

(i) the establishment of a mechanism to voluntarily report identified vulnerabilities and opportunities for improvement;

(ii) the establishment of metrics to assess the effectiveness and timeliness of the Department's and Information Sharing and Analysis Centers' information sharing capabilities; and

(iii) the establishment of a mechanism for anonymous suggestions and comments;

(F) implement an integration and analysis function to inform sector planning, risk mitigation, and operational activities regarding the protection of each critical infrastructure sector from cyber incidents;

(G) combine consequence, vulnerability, and threat information to share actionable assessments of critical infrastructure sector risks from cyber incidents;

(H) coordinate with the Department, the relevant Sector Specific Agency, and the relevant Sector Coordinating Council to update, maintain, and exercise the National Cybersecurity Incident Response Plan in accordance with section 229(b); and

(I) safeguard cyber threat information from unauthorized disclosure.

(3) *FUNDING.*—Of the amounts authorized to be appropriated for each of fiscal years 2014, 2015, and 2016 for the Cybersecurity and Communications Office of the Department, the Secretary is authorized to use not less than \$25,000,000 for any such year for operations support at the National Cybersecurity and Communications Integration Center established under section 228(a) of all recognized Information Sharing and Analysis Centers under paragraph (1) of this subsection.

(f) *CLEARANCES.*—The Secretary—

(1) shall expedite the process of security clearances under Executive Order 13549 or successor orders for appropriate representatives of Sector Coordinating Councils and the critical infrastructure sector Information Sharing and Analysis Centers; and

(2) may so expedite such processing to—

(A) appropriate personnel of critical infrastructure owners and critical infrastructure operators; and

(B) any other person as determined by the Secretary.

(g) *PUBLIC-PRIVATE COLLABORATION.*—The Secretary, in collaboration with the critical infrastructure sectors designated under sub-

section (b), such sectors' Sector Specific Agencies recognized under subsection (c), and the Sector Coordinating Councils recognized under subsection (d), shall—

(1) conduct an analysis and review of the existing public-private partnership model and evaluate how the model between the Department and critical infrastructure owners and critical infrastructure operators can be improved to ensure the Department, critical infrastructure owners, and critical infrastructure operators are equal partners and regularly collaborate on all programs and activities of the Department to protect critical infrastructure;

(2) develop and implement procedures to ensure continuous, collaborative, and effective interactions between the Department, critical infrastructure owners, and critical infrastructure operators; and

(3) ensure critical infrastructure sectors have a reasonable period for review and comment of all jointly produced materials with the Department.

(h) **PROTECTION OF FEDERAL CIVILIAN INFORMATION SYSTEMS.**—

(1) **IN GENERAL.**—The Secretary shall administer the operational information security activities and functions to protect and ensure the resiliency of all Federal civilian information systems.

(2) **ROLES AND RESPONSIBILITIES.**—The Secretary, in coordination with the heads of other Federal civilian agencies, shall—

(A) develop, issue, and oversee the implementation and compliance of all operational information security policies and procedures to protect and ensure the resiliency of Federal civilian information systems;

(B) administer Federal Government-wide efforts to develop and provide adequate, risk-based, cost-effective, and technology neutral information security capabilities;

(C) establish and sustain continuous diagnostics systems for Federal civilian information systems to aggregate data and identify and prioritize the mitigation of cyber vulnerabilities in such systems for cybersecurity purposes;

(D) develop, acquire, and operate an integrated and consolidated system of intrusion detection, analytics, intrusion prevention, and other information sharing and protective capabilities to defend Federal civilian information systems from cyber threats;

(E) develop and conduct targeted risk assessments and operational evaluations of Federal civilian information systems, in consultation with government and private entities that own and operate such information systems, including threat, vulnerability, and impact assessments and penetration testing;

(F) develop and provide technical assistance and cyber incident response capabilities to secure and ensure the resilience of Federal civilian information systems;

(G) review annually the operational information security activities and functions of each of the Federal civilian agencies;

(H) develop minimum technology neutral operational requirements for network and security operations centers to

facilitate the protection of all Federal civilian information systems;

(I) develop reporting requirements, consistent with relevant law, to ensure the National Cybersecurity and Communications Integration Center established pursuant to section 228 receives all actionable cyber threat information identified on Federal civilian information systems;

(J) develop technology neutral performance requirements and metrics for the security of Federal civilian information systems;

(K) implement training requirements that include industry recognized certifications to ensure that Federal civilian agencies are able to fully and timely comply with policies and procedures issued by the Secretary under this subsection; and

(L) develop training requirements regarding privacy, civil rights, civil liberties, and information oversight for information security employees who operate Federal civilian information systems.

(3) USE OF CERTAIN COMMUNICATIONS.—

(A) IN GENERAL.—The Secretary may enter into contracts or other agreements, or otherwise request and obtain, in accordance with applicable law, the assistance of private entities that provide electronic communication services, remote computing services, or cybersecurity services to acquire, intercept, retain, use, and disclose communications and other system traffic, deploy countermeasures, or otherwise operate protective capabilities in accordance with subparagraphs (C), (D), (E), and (F) of paragraph (2). No cause of action shall exist against private entities for assistance provided to the Secretary in accordance with this subsection.

(B) RULE OF CONSTRUCTION.—Nothing in subparagraph (A) may be construed to—

(i) require or compel any private entity to enter in a contract or agreement described in such subparagraph; or

(ii) authorize the Secretary to take any action with respect to any communications or system traffic transiting or residing on any information system or network of information systems other than a Federal civilian information system.

(i) RECOMMENDATIONS REGARDING NEW AGREEMENTS.—Not later than 180 days after the date of the enactment of this section, the Secretary shall submit to the appropriate congressional committees recommendations on how to expedite the implementation of information sharing agreements for cybersecurity purposes between the Secretary and critical information owners and critical infrastructure operators and other private entities. Such recommendations shall address the development and utilization of a scalable form that retains all privacy and other protections in such agreements in existence as of such date, including Cooperative and Research Development Agreements. Such recommendations should also include any additional authorities or resources that may be needed to carry out the implementation of any such new agreements.

(j) *RULE OF CONSTRUCTION.*—No provision of this title may be construed as modifying, limiting, or otherwise affecting the authority of any other Federal agency under any other provision of law.

SEC. 228. NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.

(a) *ESTABLISHMENT.*—There is established in the Department the National Cybersecurity and Communications Integration Center (referred to in this section as the “Center”), which shall be a Federal civilian information sharing interface that provides shared situational awareness to enable real-time, integrated, and operational actions across the Federal Government, and share cyber threat information by and among Federal, State, and local government entities, Information Sharing and Analysis Centers, private entities, and critical infrastructure owners and critical infrastructure operators that have an information sharing relationship with the Center.

(b) *COMPOSITION.*—The Center shall include each of the following entities:

(1) At least one Information Sharing and Analysis Center established under section 227(e) for each critical infrastructure sector.

(2) The Multi-State Information Sharing and Analysis Center to collaborate with State and local governments.

(3) The United States Computer Emergency Readiness Team to coordinate cyber threat information sharing, proactively manage cyber risks to the United States, collaboratively respond to cyber incidents, provide technical assistance to information system owners and operators, and disseminate timely notifications regarding current and potential cyber threats and vulnerabilities.

(4) The Industrial Control System Cyber Emergency Response Team to coordinate with industrial control systems owners and operators and share industrial control systems-related security incidents and mitigation measures.

(5) The National Coordinating Center for Telecommunications to coordinate the protection, response, and recovery of national security emergency communications.

(6) Such other Federal, State, and local government entities, private entities, organizations, or individuals as the Secretary may consider appropriate that agree to be included.

(c) *CYBER INCIDENT.*—In the event of a cyber incident, the Secretary may grant the entities referred to in subsection (a) immediate temporary access to the Center as a situation may warrant.

(d) *ROLES AND RESPONSIBILITIES.*—The Center shall—

(1) promote ongoing multi-directional sharing by and among the entities referred to in subsection (a) of timely and actionable cyber threat information and analysis on a real-time basis that includes emerging trends, evolving threats, incident reports, intelligence information, risk assessments, and best practices;

(2) coordinate with other Federal agencies to streamline and reduce redundant reporting of cyber threat information;

(3) provide, upon request, timely technical assistance and crisis management support to Federal, State, and local government entities and private entities that own or operate information systems or networks of information systems to protect from, prevent, mitigate, respond to, and recover from cyber incidents;

(4) *facilitate cross-sector coordination and sharing of cyber threat information to prevent related or consequential impacts to other critical infrastructure sectors;*

(5) *collaborate and facilitate discussions with Sector Coordinating Councils, Information Sharing and Analysis Centers, Sector Specific Agencies, and relevant critical infrastructure sectors on the development of prioritized Federal response efforts, if necessary, to support the defense and recovery of critical infrastructure from cyber incidents;*

(6) *collaborate with the Sector Coordinating Councils, Information Sharing and Analysis Centers, Sector Specific Agencies, and the relevant critical infrastructure sectors on the development and implementation of procedures to support technology neutral real-time information sharing capabilities and mechanisms;*

(7) *collaborate with the Sector Coordinating Councils, Information Sharing and Analysis Centers, Sector Specific Agencies, and the relevant critical infrastructure sectors to identify requirements for data and information formats and accessibility, system interoperability, and redundant systems and alternative capabilities in the event of a disruption in the primary information sharing capabilities and mechanisms at the Center;*

(8) *within the scope of relevant treaties, cooperate with international partners to share information and respond to cyber incidents;*

(9) *safeguard sensitive cyber threat information from unauthorized disclosure;*

(10) *require other Federal civilian agencies to—*

(A) *send reports and information to the Center about cyber incidents, threats, and vulnerabilities affecting Federal civilian information systems and critical infrastructure systems and, in the event a private vendor product or service of such an agency is so implicated, the Center shall first notify such private vendor of the vulnerability before further disclosing such information;*

(B) *provide to the Center cyber incident detection, analysis, mitigation, and response information; and*

(C) *immediately send and disclose to the Center cyber threat information received by such agencies;*

(11) *perform such other duties as the Secretary may require to facilitate a national effort to strengthen and maintain secure, functioning, and resilient critical infrastructure from cyber threats;*

(12) *implement policies and procedures to—*

(A) *provide technical assistance to Federal civilian agencies to prevent and respond to data breaches involving unauthorized acquisition or access of personally identifiable information that occur on Federal civilian information systems;*

(B) *require Federal civilian agencies to notify the Center about data breaches involving unauthorized acquisition or access of personally identifiable information that occur on Federal civilian information systems not later than two business days after the discovery of such a breach; and*

(C) require Federal civilian agencies to notify all potential victims of a data breach involving unauthorized acquisition or access of personally identifiable information that occur on Federal civilian information systems without unreasonable delay consistent with the needs of law enforcement; and

(13) participate in exercises run by the Department's National Exercise Program, where appropriate.

(e) *INTEGRATION AND ANALYSIS.*—The Center, in coordination with the Office of Intelligence and Analysis of the Department, shall maintain an integration and analysis function, which shall —

(1) integrate and analyze all cyber threat information received from other Federal agencies, State and local governments, Information Sharing and Analysis Centers, private entities, critical infrastructure owners, and critical infrastructure operators, and share relevant information in near real-time;

(2) on an ongoing basis, assess and evaluate consequence, vulnerability, and threat information to share with the entities referred to in subsection (a) actionable assessments of critical infrastructure sector risks from cyber incidents and to assist critical infrastructure owners and critical infrastructure operators by making recommendations to facilitate continuous improvements to the security and resiliency of the critical infrastructure of the United States;

(3) facilitate cross-sector integration, identification, and analysis of key interdependencies to prevent related or consequential impacts to other critical infrastructure sectors;

(4) collaborate with the Information Sharing and Analysis Centers to tailor the analysis of information to the specific characteristics and risk to a relevant critical infrastructure sector; and

(5) assess and evaluate consequence, vulnerability, and threat information regarding cyber incidents in coordination with the Office of Emergency Communications of the Department to help facilitate continuous improvements to the security and resiliency of public safety communications networks.

(f) *REPORT OF CYBER ATTACKS AGAINST FEDERAL GOVERNMENT NETWORKS.*—The Secretary shall submit to the Committee on Homeland Security of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Comptroller General of the United States an annual report that summarizes major cyber incidents involving Federal civilian agency information systems and provides aggregate statistics on the number of breaches, the extent of any personally identifiable information that was involved, the volume of data exfiltrated, the consequential impact, and the estimated cost of remedying such breaches.

(g) *REPORT ON THE OPERATIONS OF THE CENTER.*—The Secretary, in consultation with the Sector Coordinating Councils and appropriate Federal Government entities, shall submit to the Committee on Homeland Security of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Comptroller General of the United States an annual report on—

(1) *the capability and capacity of the Center to carry out its cybersecurity mission in accordance with this section, and sections 226, 227, 229, 230, 230A, and 230B;*

(2) *the extent to which the Department is engaged in information sharing with each critical infrastructure sector designated under section 227(b), including—*

(A) *the extent to which each such sector has representatives at the Center; and*

(B) *the extent to which critical infrastructure owners and critical infrastructure operators of each critical infrastructure sector participate in information sharing at the Center;*

(3) *the volume and range of activities with respect to which the Secretary collaborated with the Sector Coordinating Councils and the Sector-Specific Agencies to promote greater engagement with the Center; and*

(4) *the volume and range of voluntary technical assistance sought and provided by the Department to each critical infrastructure owner and critical infrastructure operator.*

SEC. 229. CYBER INCIDENT RESPONSE AND TECHNICAL ASSISTANCE.

(a) *IN GENERAL.—The Secretary shall establish Cyber Incident Response Teams to—*

(1) *upon request, provide timely technical assistance and crisis management support to Federal, State, and local government entities, private entities, and critical infrastructure owners and critical infrastructure operators involving cyber incidents affecting critical infrastructure; and*

(2) *upon request, provide actionable recommendations on security and resilience measures and countermeasures to Federal, State, and local government entities, private entities, and critical infrastructure owners and critical infrastructure operators prior to, during, and after cyber incidents.*

(b) *COORDINATION.—In carrying out subsection (a), the Secretary shall coordinate with the relevant Sector Specific Agencies, if applicable.*

(c) *CYBER INCIDENT RESPONSE PLAN.—The Secretary, in coordination with the Sector Coordinating Councils, Information Sharing and Analysis Centers, and Federal, State, and local governments, shall develop, regularly update, maintain, and exercise a National Cybersecurity Incident Response Plan which shall—*

(1) *include effective emergency response plans associated with cyber threats to critical infrastructure, information systems, or networks of information systems;*

(2) *ensure that such National Cybersecurity Incident Response Plan can adapt to and reflect a changing cyber threat environment, and incorporate best practices and lessons learned from regular exercises, training, and after-action reports; and*

(3) *facilitate discussions on the best methods for developing innovative and useful cybersecurity exercises for coordinating between the Department and each of the critical infrastructure sectors designated under section 227(b).*

(d) *UPDATE TO CYBER INCIDENT ANNEX TO THE NATIONAL RESPONSE FRAMEWORK.—The Secretary, in coordination with the heads of other Federal agencies and in accordance with the National Cybersecurity Incident Response Plan under subsection (c),*

shall regularly update, maintain, and exercise the Cyber Incident Annex to the National Response Framework of the Department.

SEC. 230. PUBLIC-PRIVATE COLLABORATION ON CYBERSECURITY.

(a) MEETINGS.—The Secretary shall meet with the Sector Coordinating Council for each critical infrastructure sector designated under section 227(b) on a biannual basis to discuss the cybersecurity threat to critical infrastructure, voluntary activities to address cybersecurity, and ideas to improve the public-private partnership to enhance cybersecurity, in which the Secretary shall—

(1) provide each Sector Coordinating Council an assessment of the cybersecurity threat to each critical infrastructure sector designated under section 227(b), including information relating to—

(A) any actual or assessed cyber threat, including a consideration of adversary capability and intent, preparedness, target attractiveness, and deterrence capabilities;

(B) the extent and likelihood of death, injury, or serious adverse effects to human health and safety caused by an act of terrorism or other disruption, destruction, or unauthorized use of critical infrastructure;

(C) the threat to national security caused by an act of terrorism or other disruption, destruction, or unauthorized use of critical infrastructure; and

(D) the harm to the economy that would result from an act of terrorism or other disruption, destruction, or unauthorized use of critical infrastructure; and

(2) provide recommendations, which may be voluntarily adopted, on ways to improve cybersecurity of critical infrastructure.

(b) REPORT.—

(1) IN GENERAL.—Starting 30 days after the end of the fiscal year in which the National Cybersecurity and Critical Infrastructure Protection Act of 2013 is enacted and annually thereafter, the Secretary shall submit to the appropriate congressional committees a report on the state of cybersecurity for each critical infrastructure sector designated under section 227(b) based on discussions between the Department and the Sector Coordinating Council in accordance with subsection (a) of this section. The Secretary shall maintain a public copy of each report, and each report may include a non-public annex for proprietary, business-sensitive information, or other sensitive information. Each report shall include, at a minimum information relating to—

(A) the risk to each critical infrastructure sector, including known cyber threats, vulnerabilities, and potential consequences;

(B) the extent and nature of any cybersecurity incidents during the previous year, including the extent to which cyber incidents jeopardized or imminently jeopardized information systems;

(C) the current status of the voluntary, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to reduce cyber risks within each critical infrastructure sector; and

(D) the volume and range of voluntary technical assistance sought and provided by the Department to each critical infrastructure sector.

(2) **SECTOR COORDINATING COUNCIL RESPONSE.**—Before making public and submitting each report required under paragraph (1), the Secretary shall provide a draft of each report to the Sector Coordinating Council for the critical infrastructure sector covered by each such report. The Sector Coordinating Council at issue may provide to the Secretary a written response to such report within 45 days of receiving the draft. If such Sector Coordinating Council provides a written response, the Secretary shall include such written response in the final version of each report required under paragraph (1).

(c) **LIMITATION.**—Information shared with or provided to a Sector Coordinating Council, a critical infrastructure sector, or the Secretary for the purpose of the activities under subsections (a) and (b) may not be used by any Federal, State, or local government department or agency to regulate the activity of any private entity.

SEC. 230A. CYBERSECURITY OCCUPATION CATEGORIES, WORKFORCE ASSESSMENT, AND STRATEGY.

(a) **SHORT TITLE.**—This section may be cited as the “Homeland Security Cybersecurity Boots-on-the-Ground Act”.

(b) **CYBERSECURITY OCCUPATION CATEGORIES.**—

(1) **IN GENERAL.**—Not later than 90 days after the date of the enactment of this section, the Secretary shall develop and issue comprehensive occupation categories for individuals performing activities in furtherance of the cybersecurity mission of the Department.

(2) **APPLICABILITY.**—The Secretary shall ensure that the comprehensive occupation categories issued under paragraph (1) are used throughout the Department and are made available to other Federal agencies.

(c) **CYBERSECURITY WORKFORCE ASSESSMENT.**—

(1) **IN GENERAL.**—Not later than 180 days after the date of the enactment of this section and annually thereafter, the Secretary shall assess the readiness and capacity of the workforce of the Department to meet its cybersecurity mission.

(2) **CONTENTS.**—The assessment required under paragraph (1) shall, at a minimum, include the following:

(A) Information where cybersecurity positions are located within the Department, specified in accordance with the cybersecurity occupation categories issued under subsection (b).

(B) Information on which cybersecurity positions are—

(i) performed by—

(I) permanent full time departmental employees, together with demographic information about such employees’ race, ethnicity, gender, disability status, and veterans status;

(II) individuals employed by independent contractors; and

(III) individuals employed by other Federal agencies, including the National Security Agency; and

(ii) vacant.

(C) *The number of individuals hired by the Department pursuant to the authority granted to the Secretary in 2009 to permit the Secretary to fill 1,000 cybersecurity positions across the Department over a three year period, and information on what challenges, if any, were encountered with respect to the implementation of such authority.*

(D) *Information on vacancies within the Department's cybersecurity supervisory workforce, from first line supervisory positions through senior departmental cybersecurity positions.*

(E) *Information on the percentage of individuals within each cybersecurity occupation category who received essential training to perform their jobs, and in cases in which such training is not received, information on what challenges, if any, were encountered with respect to the provision of such training.*

(F) *Information on recruiting costs incurred with respect to efforts to fill cybersecurity positions across the Department in a manner that allows for tracking of overall recruiting and identifying areas for better coordination and leveraging of resources within the Department.*

(d) **WORKFORCE STRATEGY.**—

(1) **IN GENERAL.**—*Not later than 180 days after the date of the enactment of this section, the Secretary shall develop, maintain, and, as necessary, update, a comprehensive workforce strategy that enhances the readiness, capacity, training, recruitment, and retention of the cybersecurity workforce of the Department.*

(2) **CONTENTS.**—*The comprehensive workforce strategy developed under paragraph (1) shall include—*

(A) *a multiphased recruitment plan, including relating to experienced professionals, members of disadvantaged or underserved communities, the unemployed, and veterans;*

(B) *a 5-year implementation plan;*

(C) *a 10-year projection of the Department's cybersecurity workforce needs; and*

(D) *obstacles impeding the hiring and development of a cybersecurity workforce at the Department.*

(e) **INFORMATION SECURITY TRAINING.**—*Not later than 270 days after the date of the enactment of this section, the Secretary shall establish and maintain a process to verify on an ongoing basis that individuals employed by independent contractors who serve in cybersecurity positions at the Department receive initial and recurrent information security training comprised of general security awareness training necessary to perform their job functions, and role-based security training that is commensurate with assigned responsibilities. The Secretary shall maintain documentation to ensure that training provided to an individual under this subsection meets or exceeds requirements for such individual's job function.*

(f) **UPDATES.**—*The Secretary shall submit to the appropriate congressional committees annual updates regarding the cybersecurity workforce assessment required under subsection (c), information on the progress of carrying out the comprehensive workforce strategy developed under subsection (d), and information on the status of the*

implementation of the information security training required under subsection (e).

(g) *GAO STUDY.*—The Secretary shall provide the Comptroller General of the United States with information on the cybersecurity workforce assessment required under subsection (c) and progress on carrying out the comprehensive workforce strategy developed under subsection (d). The Comptroller General shall submit to the Secretary and the appropriate congressional committees a study on such assessment and strategy.

(h) *CYBERSECURITY FELLOWSHIP PROGRAM.*—Not later than 120 days after the date of the enactment of this section, the Secretary shall submit to the appropriate congressional committees a report on the feasibility of establishing a Cybersecurity Fellowship Program to offer a tuition payment plan for undergraduate and doctoral candidates who agree to work for the Department for an agreed-upon period of time.

SEC. 230B. PERSONNEL AUTHORITIES.

(a) *IN GENERAL.*—

(1) *PERSONNEL AUTHORITIES.*—The Secretary may exercise with respect to qualified employees of the Department the same authority that the Secretary of Defense has with respect to civilian intelligence personnel and the scholarship program under sections 1601, 1602, 1603, and 2200a of title 10, United States Code, to establish as positions in the excepted service, appoint individuals to such positions, fix pay, and pay a retention bonus to any employee appointed under this section if the Secretary determines that such is needed to retain essential personnel. Before announcing the payment of a bonus under this paragraph, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a written explanation of such determination. Such authority shall be exercised—

(A) to the same extent and subject to the same conditions and limitations that the Secretary of Defense may exercise such authority with respect to civilian intelligence personnel of the Department of Defense; and

(B) in a manner consistent with the merit system principles set forth in section 2301 of title 5, United States Code.

(2) *CIVIL SERVICE PROTECTIONS.*—Sections 1221 and 2302, and chapter 75 of title 5, United States Code, shall apply to the positions established pursuant to the authorities provided under paragraph (1).

(3) *PLAN FOR EXECUTION OF AUTHORITIES.*—Not later than 120 days after the date of the enactment of this section, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report that contains a plan for the use of the authorities provided under this subsection.

(b) *ANNUAL REPORT.*—Not later than one year after the date of the enactment of this section and annually thereafter for four years, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Secu-

riety and Governmental Affairs of the Senate a detailed report (including appropriate metrics on actions occurring during the reporting period) that discusses the processes used by the Secretary in implementing this section and accepting applications, assessing candidates, ensuring adherence to veterans' preference, and selecting applicants for vacancies to be filled by a qualified employee.

(c) *DEFINITION OF QUALIFIED EMPLOYEE.*—In this section, the term “qualified employee” means an employee who performs functions relating to the security of Federal civilian information systems, critical infrastructure information systems, or networks of either of such systems.

* * * * *

SUPPORT ANTI-TERRORISM BY FOSTERING EFFECTIVE TECHNOLOGIES ACT OF 2002

* * * * *

TITLE VIII—COORDINATION WITH NON-FEDERAL ENTITIES; INSPECTOR GENERAL; UNITED STATES SECRET SERVICE; COAST GUARD; GENERAL PROVISIONS

* * * * *

Subtitle G—Support Anti-terrorism by Fostering Effective Technologies Act of 2002

* * * * *

SEC. 862. ADMINISTRATION.

(a) * * *

(b) **[DESIGNATION OF QUALIFIED ANTI-TERRORISM TECHNOLOGIES]** *DESIGNATION OF ANTI-TERRORISM AND CYBERSECURITY TECHNOLOGIES.*—The Secretary may designate anti-terrorism and cybersecurity technologies that qualify for protection under the system of risk management set forth in this subtitle in accordance with criteria that shall include, but not be limited to, the following:

(1) * * *

* * * * *

(3) Existence of extraordinarily large or extraordinarily unquantifiable potential third party liability risk exposure to the Seller or other provider of such anti-terrorism or cybersecurity technology.

(4) Substantial likelihood that such anti-terrorism or cybersecurity technology will not be deployed unless protections under the system of risk management provided under this subtitle are extended.

(5) Magnitude of risk exposure to the public if such anti-terrorism *or cybersecurity* technology is not deployed.

* * * * *

(7) Anti-terrorism technology *or cybersecurity technology* that would be effective in facilitating the defense against acts of terrorism *or qualifying cyber incidents*, including technologies that prevent, defeat or respond to such acts.

* * * * *

SEC. 863. LITIGATION MANAGEMENT.

(a) FEDERAL CAUSE OF ACTION.—

(1) IN GENERAL.—There shall exist a Federal cause of action for claims arising out of, relating to, or resulting from an act of terrorism *or qualifying cyber incident* when qualified anti-terrorism *or cybersecurity* technologies have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the Seller. The substantive law for decision in any such action shall be derived from the law, including choice of law principles, of the State in which such acts of terrorism *or qualifying cyber incidents* occurred, unless such law is inconsistent with or preempted by Federal law. Such Federal cause of action shall be brought only for claims for injuries that are proximately caused by sellers that provide qualified anti-terrorism *or cybersecurity* technology to Federal and non-Federal government customers.

(2) JURISDICTION.—Such appropriate district court of the United States shall have original and exclusive jurisdiction over all actions for any claim for loss of property, personal injury, or death arising out of, relating to, or resulting from an act of terrorism *or qualifying cyber incident* when qualified anti-terrorism *or cybersecurity* technologies have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the Seller.

* * * * *

(c) COLLATERAL SOURCES.—Any recovery by a plaintiff in an action under this section shall be reduced by the amount of collateral source compensation, if any, that the plaintiff has received or is entitled to receive as a result of such acts of terrorism *or qualifying cyber incidents* that result or may result in loss to the Seller.

(d) GOVERNMENT CONTRACTOR DEFENSE.—

(1) IN GENERAL.—Should a product liability or other lawsuit be filed for claims arising out of, relating to, or resulting from an act of terrorism *or qualifying cyber incident* when qualified anti-terrorism *or cybersecurity* technologies approved by the Secretary, as provided in paragraphs (2) and (3) of this subsection, have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the Seller, there shall be a rebuttable presumption that the government contractor defense applies in such lawsuit. This presumption shall only be overcome by evidence showing that the Seller acted fraudulently or with willful misconduct in submitting information to the Secretary during the course of the Secretary's consideration of such technology under this subsection. This presumption of the government contractor de-

fense shall apply regardless of whether the claim against the Seller arises from a sale of the product to Federal Government or non-Federal Government customers.

(2) EXCLUSIVE RESPONSIBILITY.—The Secretary will be exclusively responsible for the review and approval of anti-terrorism or cybersecurity technology for purposes of establishing a government contractor defense in any product liability lawsuit for claims arising out of, relating to, or resulting from an act of terrorism or *qualifying cyber incident* when qualified anti-terrorism or cybersecurity technologies approved by the Secretary, as provided in this paragraph and paragraph (3), have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the Seller. Upon the Seller's submission to the Secretary for approval of anti-terrorism or cybersecurity technology, the Secretary will conduct a comprehensive review of the design of such technology and determine whether it will perform as intended, conforms to the Seller's specifications, and is safe for use as intended. The Seller will conduct safety and hazard analyses on such technology and will supply the Secretary with all such information.

(3) CERTIFICATE.—For anti-terrorism or cybersecurity technology reviewed and approved by the Secretary, the Secretary will issue a certificate of conformance to the Seller and place the anti-terrorism or cybersecurity technology on an Approved Product List for Homeland Security.

(e) EXCLUSION.—Nothing in this section shall in any way limit the ability of any person to seek any form of recovery from any person, government, or other entity that—

(1) attempts to commit, knowingly participates in, aids and abets, or commits any act of terrorism or *qualifying cyber incident*, or any criminal act related to or resulting from such act of terrorism or *qualifying cyber incident*; or

(2) participates in a conspiracy to commit any such act of terrorism or *qualifying cyber incident* or any such criminal act.

SEC. 864. RISK MANAGEMENT.

(a) IN GENERAL.—

(1) LIABILITY INSURANCE REQUIRED.—Any person or entity that sells or otherwise provides a qualified anti-terrorism or cybersecurity technology to Federal and non-Federal Government customers ("Seller") shall obtain liability insurance of such types and in such amounts as shall be required in accordance with this section and certified by the Secretary to satisfy otherwise compensable third-party claims arising out of, relating to, or resulting from an act of terrorism or *qualifying cyber incident* when qualified anti-terrorism or cybersecurity technologies have been deployed in defense against or response or recovery from such act.

(2) MAXIMUM AMOUNT.—For the total claims related to 1 such act of terrorism or *qualifying cyber incident*, the Seller is not required to obtain liability insurance of more than the maximum amount of liability insurance reasonably available from private sources on the world market at prices and terms that will not unreasonably distort the sales price of Seller's anti-terrorism or cybersecurity technologies.

(3) SCOPE OF COVERAGE.—Liability insurance obtained pursuant to this subsection shall, in addition to the Seller, protect the following, to the extent of their potential liability for involvement in the manufacture, qualification, sale, use, or operation of qualified anti-terrorism *or cybersecurity* technologies deployed in defense against or response or recovery from an act of terrorism *or qualifying cyber incident*:

(A) * * *

* * * * *

(4) THIRD PARTY CLAIMS.—Such liability insurance under this section shall provide coverage against third party claims arising out of, relating to, or resulting from the sale or use of anti-terrorism *or cybersecurity* technologies.

(b) RECIPROCAL WAIVER OF CLAIMS.—The Seller shall enter into a reciprocal waiver of claims with its contractors, subcontractors, suppliers, vendors and customers, and contractors and subcontractors of the customers, involved in the manufacture, sale, use or operation of qualified anti-terrorism *or cybersecurity* technologies, under which each party to the waiver agrees to be responsible for losses, including business interruption losses, that it sustains, or for losses sustained by its own employees resulting from an activity resulting from an act of terrorism *or qualifying cyber incident* when qualified anti-terrorism *or cybersecurity* technologies have been deployed in defense against or response or recovery from such act.

(c) EXTENT OF LIABILITY.—Notwithstanding any other provision of law, liability for all claims against a Seller arising out of, relating to, or resulting from an act of terrorism *or qualifying cyber incident* when qualified anti-terrorism *or cybersecurity* technologies have been deployed in defense against or response or recovery from such act and such claims result or may result in loss to the Seller, whether for compensatory or punitive damages or for contribution or indemnity, shall not be in an amount greater than the limits of liability insurance coverage required to be maintained by the Seller under this section.

SEC. 865. DEFINITIONS.

For purposes of this subtitle, the following definitions apply:

(1) QUALIFIED ANTI-TERRORISM *OR CYBERSECURITY* TECHNOLOGY.—For purposes of this subtitle, the term “qualified anti-terrorism *or cybersecurity* technology” means any product, equipment, service (including support services), device, or technology (including information technology) designed, developed, modified, or procured for the specific purpose of preventing, detecting, identifying, or deterring acts of terrorism *or qualifying cyber incidents* or limiting the harm such acts *or incidents* might otherwise cause, that is designated as such by the Secretary.

* * * * *

(7) QUALIFYING CYBER INCIDENT.—

(A) *IN GENERAL.*—The term “qualifying cyber incident” means any act that the Secretary determines meets the requirements under subparagraph (B), as such requirements are further defined and specified by the Secretary.

(B) *REQUIREMENTS.*—A qualifying cyber incident meets the requirements of this subparagraph if—

(i) the incident is unlawful or otherwise exceeds authorized access authority;

(ii) the incident disrupts or imminently jeopardizes the integrity, operation, confidentiality, or availability of programmable electronic devices, communication networks, including hardware, software and data that are essential to their reliable operation, electronic storage devices, or any other information system, or the information that system controls, processes, stores, or transmits;

(iii) the perpetrator of the incident gains access to an information system or a network of information systems resulting in—

(I) misappropriation or theft of data, assets, information, or intellectual property;

(II) corruption of data, assets, information, or intellectual property;

(III) operational disruption; or

(IV) an adverse effect on such system or network, or the data, assets, information, or intellectual property contained therein; and

(iv) the incident causes harm inside or outside the United States that results in material levels of damage, disruption, or casualties severely affecting the United States population, infrastructure, economy, or national morale, or Federal, State, local, or tribal government functions.

(C) *RULE OF CONSTRUCTION.*—For purposes of clause (iv) of subparagraph (B), the term “severely” includes any qualifying cyber incident, whether at a local, regional, state, national, international, or tribal level, that affects—

(i) the United States population, infrastructure, economy, or national morale, or

(ii) Federal, State, local, or tribal government functions.

* * * * *

COMMITTEE CORRESPONDENCE

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6301

(202) 225-6371
www.science.house.gov

February 24, 2014

The Honorable Michael McCaul
Chairman
Committee on Homeland Security
H2-176
Washington, DC 20515

Dear Chairman McCaul,

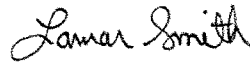
I am writing to you concerning the jurisdictional interest of the Committee on Science, Space, and Technology in H.R. 3696, the "National Cybersecurity and Critical Infrastructure Protection Act of 2013." The bill contains provisions that fall within the jurisdiction of the Committee on Science, Space, and Technology.

I recognize and appreciate the desire to bring this legislation before the House of Representatives in an expeditious manner, and accordingly, I will waive further consideration of this bill in Committee, notwithstanding any provisions that fall within the jurisdiction of the Committee on Science, Space, and Technology. This waiver, of course, is conditional on our mutual understanding that agreeing to waive consideration of this bill should not be construed as waiving, reducing, or affecting the jurisdiction of the Committee on Science, Space, and Technology.

This waiver is also given with the understanding that the Committee on Science, Space, and Technology expressly reserves its authority to seek conferees on any provision within its jurisdiction during any House-Senate conference that may be convened on this, or any similar legislation. I ask for your commitment to support any request by the Committee for conferees on H.R. 3696 as well as any similar or related legislation.

I ask that a copy of this letter and your response be included in the report on H.R. 3696 and also be placed in the Congressional Record during consideration of this bill on the House floor.

Sincerely,

A handwritten signature in black ink that reads "Lamar Smith". The signature is written in a cursive, flowing style.

Lamar Smith
Chairman
Committee on Science,
Space, and Technology

cc: The Hon. John Boehner, Speaker
The Hon. Eric Cantor, Majority Leader
The Hon. Eddie Bernice Johnson, Ranking Member, Committee on Science,
Space, and Technology
The Hon. Bennie G. Thompson, Ranking Member, Committee on Homeland
Security
Mr. Thomas J. Wickham, Jr., Parliamentarian

MICHAEL T. McCaul, TEXAS
CHAIRMAN



BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

One Hundred Thirteenth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

February 24, 2014

The Honorable Lamar Smith
Chairman
Committee on Science, Space, and Technology
2321 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Smith:

Thank you for your letter regarding H.R. 3696, the "National Cybersecurity and Critical Infrastructure Protection Act of 2014." I acknowledge your Committee's jurisdictional interest in this legislation and agree that by forgoing a sequential referral on this legislation, your Committee is not diminishing or altering its jurisdiction.

I also concur with you that forgoing action on H.R. 3696 does not in any way prejudice the Committee on Science, Space, and Technology with respect to its jurisdictional prerogatives on this bill or similar legislation in the future. I would support your effort to seek appointment of an appropriate number of conferees to any House-Senate conference involving H.R. 3696 or similar legislation.

Finally, I will include your letter and this response in the report accompanying H.R. 3696 as well as the *Congressional Record* during consideration of this bill on the House floor. I appreciate your cooperation regarding this legislation, and I look forward to working with the Committee on Science, Space, and Technology as H.R. 3696 moves through the legislative process.

Sincerely,

A handwritten signature in cursive script that reads "Michael T. McCaul".

Michael T. McCaul
Chairman

cc: The Honorable John Boehner, Speaker
The Honorable Eric Cantor, Majority Leader
The Honorable Eddie Bernice Johnson, Ranking Member, Committee on Science,
Space, and Technology
The Honorable Bennie G. Thompson, Ranking Member, Committee on Homeland
Security
Mr. Thomas J. Wickham, Jr., Parliamentarian

DARRELL E. ISSA, CALIFORNIA
CHAIRMAN

JOHN L. MICA, FLORIDA
MICHAEL R. TURNER, OHIO
JOHN J. DUNCAN, JR., TENNESSEE
PATRICK T. MCENHRY, NORTH CAROLINA
JIM JORDAN, OHIO
JASON CHAFFETZ, UTAH
TIM WALBERG, MICHIGAN
JAMES LANKFORD, OKLAHOMA
JUSTIN AMAR, MICHIGAN
PAUL A. COOPER, ARIZONA
PATRICK MEHRAN, PENNSYLVANIA
SCOTT DUKAKIS, TENNESSEE
TREV GOWDY, SOUTH CAROLINA
BLAKE FARENTHOLD, TEXAS
DOC HASTINGS, WASHINGTON
CYNTHIA M. LUMMIS, WYOMING
ROD WOODALL, GEORGIA
THOMAS RABIE, KENTUCKY
DOUG COLLINS, GEORGIA
MARK MEADOWS, NORTH CAROLINA
KERRY L. BENTVOLD, MICHIGAN
RON DESANTIS, FLORIDA

LAWRENCE J. BRADY
STAFF DIRECTOR

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States
House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5374
FACSIMILE (202) 225-5374
MINORITY (202) 225-0051
<http://oversight.house.gov>

ELIJAH E. CUMMINGS, MARYLAND
RANKING MINORITY MEMBER

CAROLYN B. MALONEY, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
JOHN F. THERRY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
STEPHEN F. LYNCH, MASSACHUSETTS
JIM COOPER, TENNESSEE
GERALD E. CONNOLLY, VIRGINIA
JACKIE SPOER, CALIFORNIA
MATTHEW A. CARTWRIGHT, PENNSYLVANIA
L. TAMMY DUCKWORTH, ILLINOIS
ROBIN L. KELLY, ILLINOIS
DANNY K. DAVIS, ILLINOIS
PETER WELCH, VERMONT
TONY CARDENAS, CALIFORNIA
STEVEN A. HORSTFORD, NEVADA
MICHELLE LUJAN GRISHAM, NEW MEXICO
VACANCY

July 23, 2014

The Honorable Michael McCaul
Chairman
Committee on Homeland Security
U.S. House of Representatives
Washington, D.C. 20515

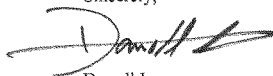
Dear Mr. Chairman:

I am writing concerning H.R. 3696, the "National Cybersecurity and Critical Infrastructure Protection Act of 2013," which your Committee reported on February 5, 2014.

H.R. 3696 contains provisions within the Committee on Oversight and Government Reform's Rule X jurisdiction. As a result of your having consulted with the Committee, and in order to expedite this bill for floor consideration, the Committee on Oversight and Government Reform will forego action on the bill, contingent on the removal of subsection (h) "Protection of Federal Civilian Information Systems," (beginning at line 17 of page 23 of the reported version). This is being done on the basis of our mutual understanding that doing so will in no way diminish or alter the jurisdiction of the Committee on Oversight and Government Reform with respect to the appointment of conferees, or to any future jurisdictional claim over the subject matters contained in the bill or similar legislation.

I would appreciate your response to this letter confirming this understanding, and would request that you include a copy of this letter and your response in the Committee Report and in the *Congressional Record* during the floor consideration of this bill. Thank you in advance for your cooperation.

Sincerely,



Darrell Issa
Chairman

cc: The Honorable John Boehner, Speaker of the House
The Honorable Bennie Thompson, Ranking Minority Member
Committee on Homeland Security
The Honorable Elijah Cummings, Ranking Minority Member
Committee on Oversight and Government Reform
Mr. Tom Wickham, Parliamentarian

MICHAEL T. McCAUL, TEXAS
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER



One Hundred Thirteenth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

July 23, 2014

The Honorable Darrell E. Issa
Chairman
Committee on Oversight and Government Reform
2157 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Issa:

Thank you for your letter regarding the Committee on the Oversight and Government Reform's jurisdictional interest in H.R. 3696, the "National Cybersecurity and Critical Infrastructure Protection Act of 2013." I acknowledge that by foregoing further action on this legislation, your Committee is not diminishing or altering its jurisdiction.

I also concur with you that forgoing action on this bill does not in any way prejudice the Committee on Oversight and Government Reform with respect to its jurisdictional prerogatives on this bill or similar legislation in the future. Moving forward, subsection (h), referred to in your letter, will be removed from H.R. 3696 prior to consideration on the House floor. As you have requested, I would support your effort to seek an appointment of an appropriate number of conferees to any House-Senate conference involving this or similar legislation.

Finally, I will include your letter and this response in the report accompanying H.R. 3696 and in the *Congressional Record* during consideration of this bill on the House floor. I appreciate your cooperation regarding this legislation, and I look forward to working with the Committee on Oversight and Government Reform as H.R. 3696 moves through the legislative process.

Sincerely,

MICHAEL T. McCAUL
Chairman

cc: The Honorable John Boehner, Speaker, U.S. House of Representatives
The Honorable Bennie Thompson, Ranking Minority Member, Committee on Homeland
Security
The Honorable Elijah Cummings, Jr. Ranking Minority Member, Committee on
Oversight and Government Reform
Mr. Tom Wickham, Jr., Parliamentarian

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED THIRTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115
Majority (201) 225-2927
Minority (201) 225-3841

July 22, 2014

The Honorable Michael T. McCaul
Chairman
Committee on Homeland Security
176 Ford House Office Building
Washington, D.C. 20515

Dear Chairman McCaul,

I write concerning H.R. 3696, the "National Cybersecurity and Critical Infrastructure Protection Act of 2014." As you are aware, the bill was referred primarily to the Committee on Homeland Security, but the Committee on Energy and Commerce has a jurisdictional interest in the bill and has requested a sequential referral.

However, given your desire to bring this legislation before the House in an expeditious manner, I will not insist on a sequential referral of H.R. 3696. I do so with the understanding that, by foregoing such a referral, the Committee on Energy and Commerce does not waive any jurisdictional claim on this or similar matters, and the Committee reserves the right to seek the appointment of conferees.

I would appreciate your response to this letter confirming this understanding, and ask that a copy of our exchange of letters on this matter be included in the *Congressional Record* during consideration of H.R. 3696 on the House floor.

Sincerely,



Fred Upton
Chairman

MICHAEL T. McCAUL, TEXAS
CHAIRMAN

RENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER



One Hundred Thirteenth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

July 23, 2014

The Honorable Fred Upton
Chairman
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Upton:

Thank you for your letter regarding the Committee on Energy and Commerce's jurisdictional interest in H.R. 3696, the "National Cybersecurity and Critical Infrastructure Protection Act of 2014." I acknowledge that by foregoing a sequential referral on this legislation, your Committee is not diminishing or altering its jurisdiction.

I also concur with you that forgoing action on this bill does not in any way prejudice the Committee on Energy and Commerce with respect to its jurisdictional prerogatives on this bill or similar legislation in the future, and I would support your effort to seek an appointment of an appropriate number of conferees to any House-Senate conference involving this or similar legislation.

Finally, I will include your letter and this response in the *Congressional Record* during consideration of this bill on the House floor. I appreciate your cooperation regarding this legislation, and I look forward to working with the Committee on Energy and Commerce as H.R. 3696 moves through the legislative process.

Sincerely,

A handwritten signature in dark ink, reading "Michael T. McCaul".

MICHAEL T. McCAUL
Chairman

cc: The Honorable John Boehner, Speaker, U.S. House of Representatives
The Honorable Eric Cantor, Majority Leader, U.S. House of Representatives
The Honorable Bennie Thompson, Ranking Minority Member, Committee on Homeland
Security
The Honorable Henry Waxman, Ranking Minority Member, Committee on Energy and
Commerce
Mr. Tom Wickham, Jr., Parliamentarian

